Department of Psychology

Predicting Individual Differences in Vulnerability to Fraud

Martina Dove

The thesis is submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy of the University of Portsmouth.

27th February 2018.

Supervised by:

Dr Mark Turner

Dr Alessandra Fasulo

Dr Darren Van Laar

General Abstract

The growing array of scams and the ability to commit fraud from different countries via the Internet makes it difficult for authorities to identify and prosecute offenders, leaving victims without justice. Fraud prevention often concentrates on warning victims about specific scams already in operation, however, such information dates quickly as new scams arise or scammers adapt their techniques. Additionally, Internet security warnings are frequently ignored due to their abundance and the security fatigue felt by users. An individual difference approach to scam prevention has not as yet been adopted by relevant agencies, despite the fact that scammers often focus on those characteristics when targeting potential victims. This approach would allow for more tailor-made advice to potential and repeat victims of fraud.

The aim of the present thesis was to identify individual differences that may be implicated in vulnerability to fraudulent offers in order to develop a valid measure of susceptibility to fraud. In the first study, semi-structured interviews were conducted with fraud victims to explore personal meanings and experiences associated with becoming a victim of fraud. Using a thematic analysis, several diverse reasons emerged for being motivated to respond to and remain engaged with fraudulent offers. These included the personal needs and attributes of the victim; their life circumstances, interpretation of source credibility and the type of persuasion techniques used. These findings, along with available research, theories and models, were used to inform the development of a psychometric measure assessing individual vulnerability to fraud in the second study. The newly developed Susceptibility to Fraud Scale consisted of five subscales measuring compliance, impulsivity, vigilance, the time invested in decision-making and belief in justice; the Scale was found to predict previous fraud victimisation, the ability to recognise phishing correspondence, and real-life situations that may be a scam. In the final study, the newly developed scale was tested using a proxy scam situation. Susceptibility to fraud evaluated by the scale was related to the acceptance of false personality feedback (known as the Barnum Effect), with individuals who were more susceptible to fraud, compliant and impulsive, more likely to see themselves as inferior to others. Previous fraud victimisation was connected to impulsivity. The findings also suggested that fraud susceptibility may not always be connected to fraud victimisation.

The newly developed Susceptibility to Fraud Scale is the first scale of its kind. It is based on the various analytical concepts and supported by the evidence of three separate studies, offering new ways of addressing vulnerability to fraud offers. Additionally, the overall findings of this programme of research were used in the formation of the proposed Model of Fraud Susceptibility.

Declaration

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

_____

Martina Dove

27th February, 2018

Thesis Word count: 68 462 words

Dedication

To grandma and grandpa Zelenić, for making my childhood magical and full of unconditional love. I miss you every single day.

Also, to my grandma in law Stella Dove. You were a shining star and I am so grateful I got to know you.

Acknowledgements

I would like to thank my supervisory team who have been through so much with me. Dr. Mark Turner, for his patience, perseverance and his perfectionism. Dr. Alessandra Fasulo, who worked very hard to develop my qualitative skills and who awakened my passion for qualitative research. And last but not least, Dr. Darren Van Laar, for great advice and kind words along the way.

Special thanks go to all my participants, especially participants who shared their painful fraud stories with me. Thank you. I know it was not easy and I hope I did them justice. Your stories have touched me deeply and made me realise how harmful fraud victimisation can be and why it is important to fight it any way we can.

There are also many people who helped me along the way, either by offering a kind word, advice or just by being an inspiration. I was lucky to be a part of a wonderful department and a wonderful university. In no particular order, I just want to thank some people who have made this journey so much easier without having to.

Prof. Alan Costall, who is one of the nicest professors I have ever come across. And always interested in everyone. Dr. Sherria Hoskins, for supportive advice on various topics. Dr. Julie Udell and Dr. Dominic Pearson, my annual reviewers who have provided great advice along the way year on year. My fellow peers, especially Niko, Dom, Gary, Gemma, Liam and Louise, who have, at times of neuroticism and stress, offered a kind word, helpful advice or just an outlet for my frustrations, thank you so much. I also want to thank Paul Marshman for the same.

I was extremely lucky to receive invaluable advice from experts in the field during the course of this journey. Prof. Stephen Lea, Prof. Stephen Greenspan, Prof. Jeff Langenderfer and Dr. Jacki Tapley, thank you for your valuable feedback and encouragement. I would also like to thank Louise Baxter from National Trading Standards, as well as different regional Trading Standards who have taken keen interest in my research. Specifically Stephen Greenfield from Suffolk County Council Trading Standards. The work you do is crucial. Also, detective Jonathan Frost and commander David Clarke at City of London police for being interested in my research, answering questions and offering support.

I also want to thank wonderful Tony Murray, fraud investigator with Durham Constabulary and talented scam tech expert Scott McGready, for endorsing fraud prevention with much passion, for the encouragement and for making me part of their scam busting family.

A big thank you to my best friend Vlatka for many years of friendship, loyalty, encouragement, devotion and laughter. And for that one time when a guy in a pub called me stupid and was then reduced to tears by the sheer strength of her arguments.

And last but not least, a big thank you to my enduring husband Ben, who bravely remains my biggest fan and who is, no doubt, eagerly awaiting the completion of this thesis.

Dissemination

Conferences

Dove, M. Turner, M and Van Laar, D. (2013). Psychological Factors in the Reduction of Susceptibility to Internet Scams. First Annual Cyberpsychology Conference, De Montfort University, Leicester, UK.

Dove, M., Turner, M., Van Laar, D. and Fasulo, A. (2015). The voices of scam victims: A psychological model of the experience of fraud. Social Networking in Cyberspace Conference, University of Wolverhampton

Dove, M., Turner, M., Van Laar, D. and Fasulo, A. (2016). Predicting individual differences in vulnerability to fraud: the development of a scam susceptibility scale. Rethinking Cybercrime Conference, University of Central Lancashire

Dove, M., Turner, M., Van Laar, D. and Fasulo, A. (2016). Predicting individual differences in vulnerability to fraud: the development of a scam susceptibility scale. Science Together: Science Postgraduate Research Conference, University of Portsmouth

Dove, M., Turner, M., Van Laar, D. and Fasulo, A. (2016). Predicting individual differences in vulnerability to fraud, Silence of the Scams: Progress, Practice and Prevention Conference, Brunel University London

Dove, M., Turner, M., Van Laar, D. and Fasulo, A. (2017). Not a victimless crime: Psychological effects of fraud victimisation, Scams; exposing the hidden danger to our health, National Trading Standards and Consumer Empowerment Alliance Conference, Jury's Inn Hotel, Birmingham, 25th- 26th April.

Seminars and presentations

Dove, M. Turner, M and Van Laar, D. (2013). Psychological Factors in the Reduction of Susceptibility to Internet Scams. Poster presentation, University of Portsmouth, UK.

Dove, M. Turner, M and Van Laar, D. Fassulo, A (2014). Individual Factors in the Reduction of Susceptibility to Internet and Face-to-Face Scams. Oral presentation, University of Portsmouth, UK.

Dove, M. Turner, M and Van Laar, D. Fassulo, A (2015). The voices of scam victims: A Psychological model of the experience of fraud, Oral presentation, University of Portsmouth, UK.

Dove, M. Turner, M and Van Laar, D. Fassulo, A (2016). Predicting individual differences in vulnerability to fraud, Oral presentation. University of Portsmouth, UK.

Dove, M. (2016). Could you spot an online scam? Seminar. University of Brighton, UK.

Contents

List of contents

List of Tables

List of Figures

Abbreviations

STFS - Susceptibility to Fraud Scale

OFT - Office of Fair Trading

UK - United Kingdom

NFA - National Fraud Authority

AFI – Annual Fraud Indicator

SFO - Serious Fraud Office

FCA - Financial Conduct Authority

CPS - Crown Prosecution Service

DVD - Digital video disc

ID - Identity

NTS -National Trading Standards

CIFAS - Credit Industry Fraud Avoidance System

CEO - Chief executive officer

VOIP - Voice Over Internet

SMS – Short Message Service

BBB - Better Business Bureau

ELM - Elaboration Likelihood Model

CRT - Cognitive Reflection Test

IQ - Intelligence quotient

IPIP - International Item Personality Pool

PTS – Propensity to Trust Survey

NEO PI-R – Revised NEO Personality Inventory

BPS - British Psychological Society

IT - Information technology

TS - Trading Standards

PHSO – Parliamentary and Health Service Ombudsman

FCA – Financial Conduct Authority

HGV - Heavy goods vehicle

URL - Uniform Resource Locator

StP – Susceptibility to Persuasion

LOC – Locus of Control

GCS – Gudjonson's (1989) Compliance Scale

SOSS - Sense of Self Scale

Chapter 1
General introduction

'And to think that, by tomorrow, instead of four gold pieces they might be a thousand, or two thousand. Why not follow my advice, and bury them in Field of Miracles?'
'Impossible, today. I'll go another time.'
'Another time will be too late', said the fox.
'Why?'
'Because a rich man has bought the field, and after tomorrow nobody will be allowed to bury his money there.' (Collodi, 2011, p.102)

1.1 Field of miracles

In the 1800s, the Italian writer Carlo Collodi wrote a fairy tale about a lovable wooden puppet, that dreams of becoming a real boy (Collodi, 2011). The book follows the adventures of the puppet as he travels. Along his journey, he comes across a cat and a fox, a pair of swindlers who manage to defraud him several times before he learns not to trust them. The wooden puppet was called Pinocchio and the fairy tale became a well-known children's story adapted many times since it was first published. However, very few people today know about the original storyline, which is rather dark at times. The fox and the cat first present themselves as a charitable pair that only wants to help Pinocchio double his golden coins by telling him about the field of miracles where, if one plants a coin, a tree full of coins grows, maximising one's investment. The fox and the cat accompany Pinocchio to the field of miracles, where they watch him plant his coins. Expecting his coin to grow into a fortune, Pinocchio finds out that the fox and the cat dug out his coins in the night and left him with nothing. These encounters are somewhat akin to scams in operation today and exhibit persuasion techniques frequently used by scammers, such as evoking greed or social norms (i.e. being helpful and kind to others who need help). Pinocchio encounters the fox and the cat again, hardly recognisable now, dishevelled and looking pitiful. To evoke sympathy, the fox and the cat pretend to be defenceless invalids, asking for help, but Pinocchio has learned his lesson and no longer trusts them. Greenspan (2009) argues that such fairy tales are an integral part of the folklore, serving as a warning about those that are out to betray our trust. It is therefore possible that these types of narratives, told through fairy tales across centuries, served as early scam prevention.

Scams are often associated with something that is ‘too good to be true’. Just like the field of miracles, they are designed to entice the victim to make an instant decision and the size of the fraud offer is often a powerful lure and deflects from rational thinking and concentrating on the negatives (Langenderfer & Shimp, 2001; Lea, Fischer & Evans, 2009). But they can be so much more. Scams can be part of complex interpersonal relationships between the victim and the perpetrator, bonds that are not easily broken and which encourage compliance (Goffman, 1952; Whitty, 2013). Specific techniques may also be used in order to persuade the victim. Goffman, (1952) argues that con artists are talented actors who systematically build social relationships,

in order to abuse them. Scams are therefore not always as obvious as the field of miracles.

1.2 Thesis overview

This programme of research set out to develop a framework for understanding factors that can protect against scam compliance by exploring the personal judgment processes of people that make them resilient to scam information, which may help safeguard against future susceptibility. Making people aware of their individual characteristics that may enhance their vulnerability to fraud prior to victimisation, may offer protection from becoming a victim of fraud.

Chapter 2 of this thesis reviews the literature relevant to fraud and fraud victimisation. It first sets out to summarise the data estimating fraud losses in recent years and discusses possible reasons for under reporting. Factors implicated in vulnerability to fraud and fraud compliance, relevant theoretical models, as well as techniques used by scammers are presented. Finally, methodology used in fraud research is considered.

Following the literature review, the thesis proceeds to present the results of three studies designed to develop and test a measure of susceptibility to fraud.

Figure 1.1 shows a schematic overview of the three studies that form part of this thesis.

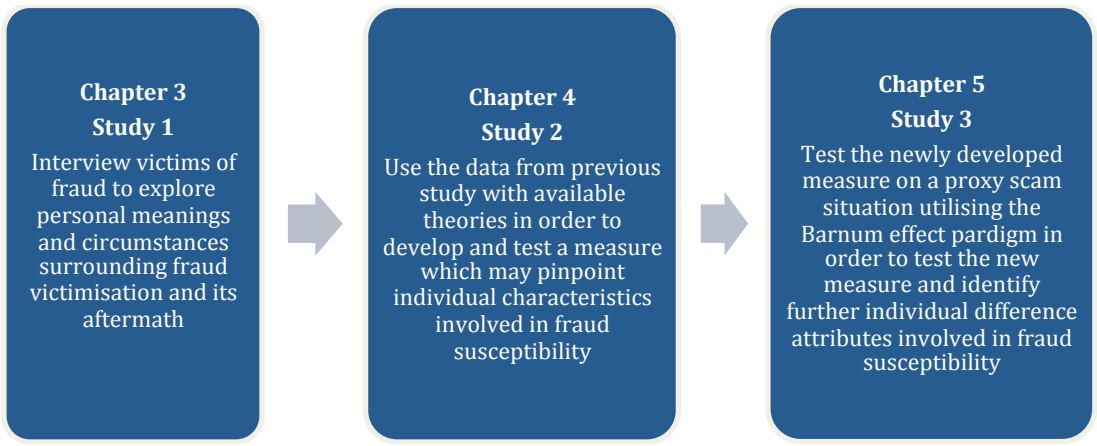


Figure 1.1 Research pathway

Chapter 3 of the thesis describes the first study in this programme of research; an interview study with victims of fraud. The purpose of this study was to explore victims' accounts of fraud victimisation and its consequences. In-depth interviews with victims of fraud were used as a suitable way of exploring the complexities of the fraud process, from victims' characteristics to the sophisticated techniques employed by perpetrators. By exploring victims' accounts in this study, underlying themes emerged that were relevant to understanding the mechanisms that underpin the fraud process. Several unique scam stages are identified and themes and subthemes relevant to each stage explored in order to inform the next stage of the research; the development of a measure that would help identify an individual's susceptibility to fraudulent communication.

Chapter 4 describes the second study, the development of a Susceptibility to Fraud Scale (STFS), a self-report questionnaire measure designed to identify personal characteristics, which might indicate a person's unique vulnerability to scams. By examining the data gathered from the previous fraud research as well as the interviews with victims of fraud in the Study 1, a questionnaire was developed, pilot tested and distributed to participants, along with a measure of Susceptibility to Persuasion (Modic & Lea, 2013), real life scenarios that may be potential fraudulent situations and examples of phishing correspondence. Data on the reliability and validity of a Susceptibility to Fraud Scale are reported. STFS responses were found to differentiate between those who had or had not previously been the victim of a scam and those that are able to recognise phishing correspondence.

Chapter 5 describes the third and final study in this programme of research. The purpose of this study was to test the newly developed measure against a proxy scam situation (i.e. the acceptance of false personality feedback) in order to evaluate its utility as a predictor of future behaviour that might be connected to susceptibility to fraud. This method was chosen as an ethical way of measuring participants' responses using simulated rather than real fraudulent attempts. Previous research of scam experiences has raised some ethical considerations, which are discussed in Chapter 2 and Chapter 5.

The newly developed measure, along with a scale measuring Compliance (Gudjonsson, 1989), used as a concurrent validity measure, and a measure of Locus of Control (Sapp & Harrod, 1993) were distributed to participants who were told they would receive personality feedback based on these measures. The same personality feedback,

consisting of neutral, negative and positive statements was then given to all participants, who were asked to rate the feedback for how accurate this was of their personality as well as how accurate it may be of people in general. STFS responses indicated that higher susceptibility to fraud was connected to greater acceptance of negative personality feedback, mostly driven by impulsivity and compliance.

The final chapter, Chapter 6, discusses the findings, limitations and implications of this research.

Fraud prevention measures are getting better at concentrating on vulnerable individuals in order to intercept fraudulent activities, however, the fraud security advice is often ignored by people due to its abundance and lack of personal touch. The present research findings offer a new way of looking at fraud vulnerability and contribute new knowledge to fraud research. The present thesis describes the construction and development of the first susceptibility to fraud measure, its usefulness and applicability to scams, and proposes the Model of Fraud Susceptibility based on the findings of this programme of research.

Chapter 2
Literature review

2.1 Fraud

The words 'scam' and 'fraud' are often used interchangeably. In their report for Office of Fair Trading (OFT), Lea et al. (2009) defined scams as 'misleading or fraudulent practices, which are widely distributed' (p. 12). On their website, Action Fraud defines fraud as; "Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person". Fraud can be committed by false representation, failing to disclose information or by abuse of position (The Fraud Act, 2006, p1). Although fraud is not a new offence, with the rise in new technologies, its delivery has become easier, allowing fraud to be committed on a larger scale than ever before. Fraud statistics show that adults between ages of 45-54 and those in higher income households are more likely to be victims of fraud than younger people or those in lower income households. Those in managerial and professional occupations were identified as more likely to be affected by fraud than full-time students, the unemployed or those in manual occupations (Office of National Statistics, 2016).

The Annual Fraud Indicator (AFI) for 2017, estimates fraud losses in the United Kingdom (UK) to be around £190 billion, with £6.8 billion lost to fraud by private individuals (Button, Gee & Mothershaw, 2017). Fraud estimates include frauds incurred in public, private and charity sectors as well as frauds incurred by private individuals. Public sector fraud includes: local and central government, tax and benefits, National Health Service and pensions. Private sector fraud includes: financial services, consumer goods, manufacturing, technology, media and telecoms, construction, retail and wholesale, travel, leisure and transportation, professional services, healthcare, pharmaceuticals and biotechnology and natural resources. Individual fraud is defined as all fraud perpetrated against private individuals (National Fraud Authority, 2010).

Fraud losses have increased rapidly since 2010, across all sectors. The true cost of individual fraud is also difficult to assess as estimates are based only on certain types of fraud and many victims of fraud choose not to report the victimisation, therefore this figure is likely to be much higher (National Fraud Authority, 2013). Table 2.1 shows the fraud estimates for the 7-year period between 2010 and 2017.

Table 2.1
Annual Fraud Indicator (AFI) estimates of losses incurred to fraud between 2010 and 2017

Annual Fraud Indicator	Public sector	Private sector	Charity sector	Individual fraud	Total
2010	£17.6	£9.3	£0.032	£3.5	£30.5
2011	£21.2	£12	£1.3	£4	£38.4
2012	£20.3	£45.5	£1.1	£6.1	£73
2013	£20.6	£21.2	£0.47	£9.1	£52
2016	£37.5	£144	£1.9	£10	£193
2017	£40.4	£140	£2.3	£6.8	£190

Note.
The values shown are in billions

No data are available for 2014 and 2015 as the National Fraud Authority (NFA), the body responsible for producing the Annual Fraud Indicator, dissolved in 2014. The Annual Fraud Indicator figures for years 2016 and 2017 were produced by collaboration of different organisations that deal with fraud (Button, et al., 2016, 2017),
The data in Table 2.1 makes it clear that fraud has been steadily increasing since 2010, with largest increases happening in the private sector.

While it is encouraging to see a reduction in total losses to fraud from 2016 to 2017, Button et al. (2017) argue this reduction may just be down to reduced levels of expenditure in certain sectors, as fraud rises with increases in expenditure. Despite apparent reductions, higher quality data indicates an increase of £2.1 billion in fraud losses from the previous year (Button et al., 2017).

2.1.1 Taxonomy of fraud

The majority of fraud research concentrates on fraud perpetrated against the government or other organisations. However, there is a lack of research when it comes to fraud perpetrated against individuals and no clear definition on how to capture information regarding fraud victimisation. This is why a fraud classification scheme was developed by the Financial Fraud Research Centre (Beals, DeLiema & Deevy, 2015), in order to systematically group and organise fraud types, preventing the overlapping, confusing definitions and characterisations developed by fraud researchers and practitioners in the absence of a better system. Beals et al. (2015) posit that a standardised coding scheme

would benefit fraud measurement by improving consistency, and allow for meaningful comparisons of results. Therefore the framework outlined key concepts and attributes that ought to be captured with regards to fraud. These include; a target, an expected benefit or outcome (e.g. investment or reward), and a specific type of fraudulent transaction (what service/product was misrepresented and in what manner). Other tags may also be applied, and these include; seriousness (categorised by the amount lost and the incident duration), victim and perpetrator characteristics, method of advertising the fraud (e.g. text message, letter, face-to-face), purchase setting (i.e. how the victim responded to the scam) and method of money transfer (e.g. credit card, cash, etc.). From these attributes, additional tags may be developed to categorise fraud further into different types of fraud; internet or cyber fraud, mail fraud, wire fraud (using a mobile phone, computer or other devices that can be used for international frauds) and policy fraud (frauds that have policy relevance, such as fraud perpetrated against the elderly). The fraud framework also outlines five framework levels, some of which consist of several sub-categories, which can be used to capture information, offering a useful tool in recording and classifying fraudulent activities.

2.1.2 Low rates of reporting

Victims of fraud are often typecast by society as naive or somehow responsible for their misfortune and frequently feel too embarrassed to report fraud or seek help (Cross, 2013; Titus & Gover, 2001; Walsh & Schram, 1980). Cross (2013) interviewed victims and near victims of the Internet fraud and found that many cite greed as a reason for complying with the requests of the scammer. Likewise, those that did not respond to fraud offers also saw fraud victims as greedy or wanting something for free. The notion of greed as a prevalent factor in fraud victimisation may be to blame for the dominant discourse of victim blaming (Cross, 2013). A study by Citizens Advice (2017) found that 72% of adults have been targeted by fraud in the past two years, yet 68% of the people targeted never tell anyone about it. The negative views of fraud victims mentioned by Cross (2013), might account for the low rates of reporting.

Another reason for low reporting might be down to not knowing whom to report different types of fraud and the belief that it is a waste of time. Research looking into attitudes of victims and repeat victims of all crime, found that low reporting rates and low victim satisfaction with reporting is particularly high among repeat victims, many of whom have no confidence in the police and feel they would not be listened to (Van

Dijk, 2001). Kerley and Copes (2002) conducted a phone fraud victimisation survey looking into fraud reporting rates and found that the reporting rates were around 22% with only 10% of one time victims and 5% of repeat victims reporting to the police. Instead participants said they reported the fraud to other official fraud reporting agencies. The strongest predictor of reporting fraud was the amount lost, with those that lost larger amounts of money reporting more readily (Kerley & Copes, 2002).

In their interviews with victims of fraud, exploring fraud support agencies, Button, Tapley and Lewis (2013) found that victims refrain from reporting fraud due to the belief that nothing would be done about it and in some cases, not knowing whom to report it to. The amount of support received by friends and family may also be implicated in how likely it is that victimisation will be reported. Research found that individuals that report fraud more frequently tend to have stronger social ties (Mason & Benson, 1996). Additionally, some fraud victims may not be aware they were defrauded, such as when donating money to a good cause or by participating in a fraudulent lottery or an investment scheme (Button, Lewis & Tapley, 2009a).

Not all frauds go unreported. Almost all identity (ID) frauds are reported (Button et al., 2009a). One explanation for this fact may be since there is no cooperation between the victim and the perpetrator; identity fraud victims may not feel as culpable as victims of other fraud types where cooperation is needed. Reporting fraud is vital in the fight against fraud. Under reporting leads to inaccurate data and difficulties in estimating the true scale of the problem. Not knowing who the fraud victims are means that there are fewer opportunities to learn from their experiences. Therefore, making sure that fraud victims get the same treatment as other crime victims is a fundamental step in encouraging them to report fraud.

2.1.3 Fraud and the justice system

Response to fraud varies depending on the agency the victim chooses to report the fraud to, such as The Police, the Office of Fair Trading, Serious Fraud Office (SFO), the Financial Services Authority (now Financial Conduct Authority or FCA), or the national or regional Trading Standards (Button, Lewis & Tapley, 2009b; Button et al., 2013). Having multiple agencies for reporting fraud often means the relevant agencies may try to pass the problem onto another agency and there is no clear, publicly available guidance on where to report different types of fraud. Additionally, victims of

fraud report not knowing where to report the fraud (Button et al., 2009b; Button et al., 2013). The launch of Action Fraud in 2009 was meant to simplify the process of reporting fraud by coordinating with the National Fraud Authority. It was also meant to address weaknesses in the support for victims of fraud, by publicising different types of fraud. The launch of Action Fraud meant that victims could no longer report fraud to the police (Loveday, 2017) and despite making the process of reporting fraud simpler, Button et al. (2013) questioned whether Action Fraud would be able to fully address the needs of fraud victims. According to Loveday (2017), the experience of fraud victims that chose to report their victimisation to Action Fraud has been substandard. Victims have received no help, they were not kept informed on the progress of their case and many cases of fraud were never passed on to the police. Many victims of fraud wish for their case to be investigated and the perpetrator to be punished, but they are often told to pursue justice through civil courts, and many do not have the funds to do so, even when they know the perpetrator. Victims defrauded online may not even be able to find out who defrauded them without an investigation; therefore, the civil route may not be viable for them (Button, et al., 2013).

Button, Lewis, Shepherd, Brooks and Wakefield (2012) looked at the numbers of prosecutions and convictions of fraud cases, supplied by the Crown Prosecution Service (CPS) and estimated that only 0.4% of frauds end in a sanction being applied, leading to a lack of deterrence and decriminalisation of fraud. They argued that, in order to deter fraud from happening, penalties for fraudulent activities must happen quickly and be inevitable, unavoidable and severe. But, this is proving difficult, as the numbers of fraud Police Officers have declined since the 1980s, resulting in lower number of frauds reported to criminal justice system (Button et al., 2012). Although Button et al. (2012) research did not seek to find out the exact number of dedicated fraud officers for England and Wales, they noted 4.2% decrease in police officers between January 2011 and January 2012, which is likely to have an impact in all areas, including fraud (also Button, Blackbourn & Tunley, 2014).

Research based on interviews and focus groups with victims of fraud indicate that it is extremely important to victims of fraud for the crime to be investigated and the perpetrator to be punished, either through custodial sentences, community orders or fines and that the punishment is not only influenced by the financial amount lost (Button et al., 2009b; Button et al., 2013; Button, McNaughton Nicholls, Kerr & Owen,

2015). Frauds that result in small losses are also less likely to be prosecuted and if caught, the perpetrator may not get a tough sentence (Button et al., 2012, Button et al., 2015). However, fraud cases that are investigated tend to be prioritised according to the amounts lost and the complexity of the fraud, which suggests that the police have a choice of which victims deserve protection, at a disadvantage of other victims (Doig, Johnson & Levi 2001).

Getting their money back is also a high priority for victims of fraud. Victims that managed to receive their money back were more satisfied as it meant that justice had been done. Where necessary, seizure of assets gained by fraud was suggested, making the perpetrator unable to profit (Button et al., 2009b; Button et al., 2013; Button et al., 2015). Finally, victims expressed a desire for restorative justice. With much of fraud being perpetrated online, anonymity means that many victims never know who committed the crime against them. An opportunity to meet the perpetrator would allow the victims to understand why they were defrauded as well as forcing the perpetrator to see the extent of the damage they had caused (Button et al., 2015).

2.1.4 Human costs of fraud

The costs associated with fraud cannot be summarised only in terms of financial loss. Titus and Gover (2001) argued that fraud often causes considerable harm to victims as it involves deception and this degrades the 'moral fibre' of the society. Despite this, the psychological effects of fraud are frequently not taken seriously and fraud victims are less likely to receive sympathy or support from others, something that is often extended to crime victims with visible injuries (Titus & Gover, 2001).

Fraud has devastating impact on the victims. Frequently, fraud victimisation affects individual's self-esteem. For example, Cross (2015) conducted interviews with elderly fraud victims and near victims and found that the discourse around fraud victimisation tends to concentrate heavily on victim blame and that even the victims themselves participated in this discourse. Many did not fully appreciate the fact that scammers utilise highly sophisticated methods in identifying and targeting vulnerable victims (Cross, 2015).

Research also found that considerable loss of funds may have detrimental effects on the quality of life as victims are left unable to afford luxuries or even food (Cross, Richards & Smith, 2016). In other cases, it may lead to bankruptcy or problems with credit

(Button et al., 2009a). Fraud may therefore, have an indirect but detrimental effect on psychological wellbeing and health through the pressure associated with money loss.

Other research, much of which is based on interviews with victims of fraud, has examined the different consequences fraud can have on victims including anger, self-blame, depression, stress, anxiety, humiliation, fear, breakdown of relationships, health problems (e.g. Button.et al., 2009a; Button, Gee, Lewis & Tapley, 2010; Button et al., 2013; Button, Lewis & Tapley, 2014; Citizens Advice, 2017; Spalek, 1999). The National Trading Standards (NTS) work with the most vulnerable victims in the UK. Based on their work with elderly fraud victims, they found that people defrauded in their own homes are at risk of dying or needing residential care within a year of the crime. They also suggested that 53% of those aged 65 and older are repeatedly targeted, leading to multiple losses, bullying or potential intimidation (National Trading Standards, 2016). In rare cases, fraud victimisation can lead to suicide. In their report on fraud trends, Cross, Smith and Richards (2014) outlined several cases where a fraud victim committed suicide following fraud victimisation.

2.1.5 Fraud prevention measures and support for victims of fraud

Fraud victimisation can be extremely harmful; therefore, it is essential that fraud prevention measures and the support offered to victims of fraud are effective. Research into support agencies for victims of fraud (Button et al., 2013), found that most of the agencies dealing with fraud offer some information on fraud and the Office of Fair Trading was previously identified as a good provider of information on fraud. It offered different types of information, from leaflets to DVDs, targeting different audiences (i.e. fraud victims, those who may become victims and those who work with victims). Its work was also proactive, frequently mimicking fraudulent offers in order to warn against fraud. As most people do not think about fraud until they are defrauded, a proactive approach may be beneficial to potential victims (Button et al., 2013). However, the Office of Fair Trading closed in 2014, which means that victims and potential victims of fraud may not be able to access quality fraud prevention advice when needed.

Support for victims of fraud also depends on whether the case reaches the courts with greatest support being offered to victims who testify in court, but even this is not always the case (Button et al., 2009b; Button et al., 2013). Police led investigations are bound

by the Victim's code of practice, which means that from an early stage, the victim is likely to have his or her needs assessed, after which they are offered enhanced support. However, the Victim's code of practice does not extend to other bodies dealing with fraud, such as local authorities, SFO or private bodies, therefore many fraud victims are left with no support from the authorities as only a small percentage of fraud cases are investigated by the police (Button et al., 2009b; Button et al., 2012). Victims of identity fraud fare better, as banks or other financial organisations that deal with that type of fraud tend to have dedicated fraud departments offering direct help to victims (Button et al., 2013). While most victims of ID fraud recoup their losses, victims of other frauds rarely do (Button, et al., 2009a), which makes effective fraud prevention fundamental in the fight against fraud.

New ways of fraud prevention are emerging. In her report on fraud prevention, Cross (2016), outlined some of the new, victim centered prevention measures implemented by the Australian authorities. These included using the financial intelligence available, such as obtaining details of people sending the funds to Nigeria and other West African countries and calling them to enquire about the details of the transactions. This intervention indicated that some of the fraud victims have been sending money for as long as a decade. These measures also included making sure that the victims are put in touch with a relevant fraud agency, removing the likelihood of victims being passed on to different agencies. This research also found that once contacted by the authorities, six out of ten victims stop sending the funds, indicating that proactive, victim orientated measures can be effective in the fight against fraud. While the preventive measures mentioned by Cross (2016) are good at identifying victims of fraud and intercepting fraudulent transactions, they do not prevent victimisation in the first place.

Scams are continually adapting to current practices and human behaviour and are becoming sophisticated and prolific, which makes developing effective and up to date warnings difficult (CIFAS, 2014; Experian, 2016). Additionally, the majority of people only take action or seek advice on how to avoid fraud after they are personally affected (Citizens Advice, 2017) and fraud warnings are often ignored, despite their abundance (Furnell & Thompson, 2009; Modic & Anderson, 2014b). Some authors have suggested that non-compliance with online security advice may be due to security fatigue (Furnell & Thompson, 2009). The time available for decision-making in the real world is often limited. When people are over-exposed to security information,

constant warnings can lead to security fatigue and therefore less caution online. Stanton, Theofanos and Prettyman (2016) argue that security warnings should, therefore, consider the complexity and amount of the existing security advice and its role in the general feelings of resignation experienced by users.

Evidence suggests that certain types of security warnings work better than others. Research by Egelman, Cranor and Hong (2008) compared the effectiveness of different phishing warnings. They found that passive phish warnings (e.g. a warning bar above the email or a single box with only an option to dismiss it) were largely ineffective. Often a bar might appear when the user is typing and is dismissed accidentally as the user is concentrating on the keyboard and not on the screen. In addition, participants who gave their details to a fraudulent website created for the purpose of the study, reported that they did so because they did not fully understand the risks. The same participants also reported they regularly ignore security warnings.

Modic and Andersen (2014b) manipulated security warnings in order to examine what would make security warnings more effective. They used existing warnings and included cues to authority (e.g. security team has identified the site is dangerous) and social influence cues (e.g. your friends have already been scammed). They also made a threat vague (e.g. a message saying access is blocked due to security concerns) or concrete (e.g. explanation of what malware does to the computer). They found that using authority and a concrete threat has a greater effect. Therefore, providing ineffective security warnings or continuous advice on new scams or scam techniques may have a counter effect, as their abundance may make people less attentive to them.

Whilst the surface details of scams may change, scams often have underlying features that are stable (Lea et al., 2009). Scam content or narratives are frequently updated to reflect current events, leaving people vulnerable to new variants even when they keep up to date with fraud prevention. For example, even the widely known Nigerian scam, in which a bank official or a solicitor contacts the victim, requesting help in getting funds out of the country, is still successful today, thanks to the new variants (Dyrud, 2005; Hiss, 2015). Fraud prevention may be more efficient if victims and potential victims were made aware not only of different scam features but also how they link with their individual characteristics, circumstances and behaviours to increase fraud vulnerability. For example, Egelman and Peer (2015) looked at individual differences

and how they impact privacy attitudes. Participants were given Need for Cognition measure (Cacioppo, Petty & Kao, 1984), General Decision Making Style measure (Scott & Bruce, 1995) and measures of risk (Blais & Weber, 2006) and privacy attitudes (Buchanan, Paine, Joinson & Reips, 2007; Malhotra, Kim & Agarwal, 2004). The study found that decision-making styles (Intuitive and Rational) and social risk-taking predicted privacy attitudes, suggesting that privacy attitudes are a result of rational decision-making and an ability to challenge social norms, but can also be down to 'gut feelings' about not wanting to share private information. Egelman and Peer (2015) conclude that privacy and security outcomes may be improved by designing the security messages around individual differences.

2.2 Scams, swindles and humbugs

In the book *The Humbugs of the World* (1866), the 19th century circus founder and hoax creator Phineas Taylor Barnum talked about scams or humbugs, as he called them, perpetrated at the time. These old-fashioned humbugs included fake lotteries, miracle cures, financial, clairvoyant and psychic scams many of which are still in operation today and are often perpetrated on the phone or online (Lea et al., 2009). The Action Fraud website's list of currently known frauds is extensive and includes among others; impersonation of officials, ticket fraud, health scams, holiday fraud, recruitment scams, rental scams, tax fraud, insurance fraud, doorstep fraud, courier fraud, pension scams, pyramid scheme fraud, inheritance scams (also Button et al., 2009a).

The diversity of frauds operating today suggests that frauds evolve quickly, proliferate and flourish in current climate and trends indicate that fraud is becoming more organised (CIFAS, 2014). With the invention of the Internet, the delivery of fraudulent offers to prospective victims became anonymous, global and more cost effective for the perpetrator (Cukier, Nesselroth & Cody 2007; Dyrud, 2005; Smith, 2010). The cross-border element, which is often part of online scams, may be responsible for the low detection and prosecution of fraud perpetrators (Button et al., 2012) and email remains the most popular delivery method for scams delivered to all age groups (Citizens Advice, 2017).

Most scams require a degree of communication and cooperation from the victim, however some frauds require none at all (Lea et al., 2009; Titus & Gover, 2001). Identity fraud victims are defrauded without any knowledge that the crime is taking place, while other scams rely on communication. For example, dating scams, work by building interpersonal trust through lengthy communication with the victim, akin to 'grooming'. This results in an emotional commitment, making it hard to refuse compliance with the requests for money (Whitty, 2013). Examples of different scams are examined below.

2.2.1 Nigerian scams

Nigerian scams (also known as advance fee or 419 scams) are a long standing, widespread and easily recognised type of scam delivered via email. For example, an email from a high-ranking Nigerian official needing help getting funds out of the country is received and victims are promised a sum of money for help with transfer of these funds (Figure 2.1). However, before this can proceed, victims are asked to pay various fees, such as legal fees (Dyrud, 2005).

FROM THE DESK OF MR KAFANDO ZIDA
DIRECTOR IN CHARGE OF AUDITING
AND ACCOUNTING SECTION
BANK OF AFRICA (B.O.A)
OUAGADOUGOU, BURKINA FASO,
WEST AFRICA.

My Dearest Friend,

I am Mr. Kafando Zida, The chief auditor in bank of Africa (boa) Burkina Faso West African, One of our customers, with his entire family was among the victims of plane crash and before his death, he has an account with us valued at $37.5 million us dollars(thirty seven million five hundred thousand u.s dollars) in our bank and according to the Burkina Faso law, at the expiration of thirteen years if nobody applies to claim the funds a grace of one year also will be given before the money will revert to the ownership of the Burkina Faso government.

My proposals is that i will like you as a foreigner to stand in as the next of kin or distant cousin for us to claim this money, so that the fruits of this old man's labour will not get into the hands of some corrupt government officials who will later use the money to sponsor war in Africa and kill innocent citizens in the search for political power.

As a foreign partner which this money will be transfer into your account, you are entitle to 40% of the total money while 55% will be for me as the moderator of this transaction and 5% will be mapped out for any expenditure that may be incur during the course of this transaction. Please note that there will be no problem as my bank has made all effort through to reach for any of his relation but all was fruitless.

My position as the chief auditor in this bank guarantees the successful execution of this (deal) transaction. Please send the following: Reply To This E-mail Address (kafandozida1@gmail.com)

1) Your full name.....
2) Sex.....
3) Age.....
4) Country.....
5) Passport or photo.....
6) Occupation.....
7) Personal Mobile number.....
8) Personal fax number.....
9) Home &office address.....

Thanks.
Mr. Kafando Zida.

Figure 2.1 Nigerian (419) advance fee scam communication

Although it is most frequently associated with the Internet, Glickman (2005) posits that Nigerian scams can be traced to the 1970s but Zuckoff (2005) argues that it goes as far back as 16th century, which shows how this type of scam has evolved through time.

Nigerian scams are often designed to appeal to emotions, evoke sympathy and often put the recipient in a position of power (i.e. a helper) and variants are common (Dyrud, 2005; Cukier et al., 2007). Recent 419 type scams tend to vary in narratives and the identities they construct, with scammers adopting either a private (e.g. war refugee, widow) or an institutional (e.g. bank official, lawyer etc.) role in order to engage the recipient and justify the contact (Hiss, 2015). Nigerian scams, which used to be delivered by postal means or via telephone and fax at a considerable cost to the scammer (Glickman, 2005) are now delivered online, incurring little cost to the scammer (Button et al., 2015).

People may often laugh at Nigerian scams as they are deemed obvious and implausible. For example, possibly the most entertaining variant of this scam is the Nigerian astronaut stranded in space and needing funds to come back home (Molloy, 2016). However, Herley (2012) argues that such scams, specifically mentioning they are from Nigeria, are used solely to identify the most gullible and vulnerable victims, whose details can then be passed on to other scammers (Nikiforova & Gregory, 2013). These victims are then repeatedly targeted. In extreme cases, Nigerian scams may end in a victim travelling to meet the scammer, being kidnapped for ransom or even killed (Cukier et al., 2007; Dyrud, 2005; Glickman, 2005). In some cases, victims have also ended up being charged with fraud themselves (Zuckoff, 2005).

2.2.2 Identity fraud and identity theft

Identity fraud involves unlawful use of an individual's personal details to get goods and services. It is often committed by redirecting victim's mail to a different address, although cases where mail is intercepted (e.g. where there is a shared hallway or letterbox) are also common. This is why frequent movers or those who live in property with shared hallway, where mail can be easily stolen are more at risk. Many victims only find out they are a victim of an identity fraud when they receive a letter chasing a debt they know nothing about (Experian, 2010; Pascoe, Owen, Keats & Gill, 2006). Perpetrators may open new bank accounts or apply for credit, take over the existing account of the victim or use the information gained to make payments online. They may also have ways of cloning credit cards (Button, et al., 2009a; Saunders &

Zucker, 1999).

More sophisticated ID fraud may include an identity theft, where a perpetrator permanently assumes the identity of the victim or someone that is deceased (Button, et al., 2009a; Rege, 2009). The new identity is often used to procure a birth certificate, passport and/or other important documents, which are needed to secure employment or large loans, such as a mortgage. This may also aid other criminal activities, such as funding terrorism (Button, et al., 2009a).

Identity fraud perpetrators often utilise publically available information, such as registrations for company directors. Information about businesses and business directors are publically available via Companies House, a website for registration of companies in the UK and can be used to add legitimacy to a scam (Button, et al., 2009a). For example, there are recent cases of a 'CEO' fraud, where the scammer contacts the company staff, pretending to be the chief executive and requesting payments to be made to fraudulent accounts (Button et al., 2017).

According to Experian (2010), the people most vulnerable to identity fraud include; company directors and business owners, individuals with successful careers, high-income earners, wealthy retired couples and young singles living in rented accommodation. Those living in London and affluent surrounding areas are also more at risk (also Pascoe et al., 2006). Romance scams can also, sometimes, lead to ID fraud (Rege, 2009). Having such a diverse range of victims makes it harder to design effective fraud protective measures fit for all.

2.2.3 Romance scams

Victims of romance scams are usually contacted through online dating sites or social media. The perpetrator develops a relationship with a victim and may claim to be in love with the victim very early on. The ensuing communication is frequent, lengthy and intense (Buchanan & Whitty, 2014). A strong bond is created by daily communication between the victim and the perpetrator, as it becomes a routine part of the victim's life. The scammer presents himself or herself as the ideal partner and grooms their victim until they are ready to be defrauded. If the victim denies a request for funds, the perpetrator may threaten to leave the relationship in order to influence compliance (Whitty, 2013).

Whitty and Buchanan (2012a) conducted interviews with victims of romance scams and examined large number of posts on an online peer support group. They found that those who held romantic beliefs, with a greater tendency to idealise romantic partners were more likely to be victims of romance scams and lose funds in the process. Men were also more likely to be victims of romance fraud than women and the likelihood did not differ for men of different sexual orientation; however, women lost more money and reported more emotional distress than men. Whitty (2013) found that romance fraud victims did not ignore the warning signs, often requesting to see proof (e.g. boarding passes they paid for) or asking the perpetrator about the country they said they were living in and trying to check facts. However, scammers often went to great lengths to present victims with fake information to make the scam look as authentic as possible.

Romance scams frequently use elaborate scenarios that vary according to the gender of the victim. For example, male fictitious characters may be presented as having a high standing such as an army general or a businessman, recently widowed and often with a child to care for. Female characters tend to be young and vulnerable and in need of help (Whitty & Buchanan, 2012a). The scam also follows a certain progression; developing trust, where the scammer may do things to prove their love with a goal of creating an intense relationship with a victim. The online relationship is often more intimate than relationships that develop face-to-face, grooming the victim for later stages of the scam (Whitty & Buchanan, 2012a; Whitty, 2013). In the grooming stage, victims are encouraged to discuss their deepest thoughts, feelings and fears, fostering trust between the perpetrator and the victim until they are ready to be defrauded. Any financial loss does not happen until after the victim has been groomed for some time. First, the perpetrator may ask for a small gift, after which a crisis occurs (e.g. the romantic partner is in a car accident) and the victim is asked for a larger sum of money. A maintenance stage may also be introduced after the crisis, where a third party is involved, in order to add plausibility, such as a doctor telling the victim that their love interest is ill and needs funds for hospital bills (Whitty & Buchanan, 2012a).

Victims often find it hard to believe the relationship is fake, even after being told by the police that they have been defrauded, which may leave them open to being defrauded again. Additionally, the impact on the victims of this type of fraud is extensive, as they

come to terms with the loss of funds as well as the loss of a relationship (Buchanan & Whitty, 2014; Whitty & Buchanan, 2012b; Whitty & Buchanan, 2016).

2.2.4 Phishing, vishing and smishing

New types of fraud and techniques that enable fraud delivery online, on the phone and via mobile phones are emerging (Kerr, Owen, McNaughton Nicholls & Button, 2013). These are outlined in Table 2.2.

Table 2.2
Some types of phishing attacks identified by Orman (2013)

Type of attack	Description
Phishing and pharming	Personal information obtained via fake websites
Smishing	Personal information obtained via SMS
Vishing	Personal information obtained over the phone
Spear phishing	Highly targeted spam emails
Koobface (social media)	Virus sent via messages on social media
Malware	Computer/smartphone taken over externally to steal personal details

Phishing is a form of social engineering attack or a request for compliance, which uses social interaction as a means to persuade (Mouton, Leenan, Malan & Venter, 2014). It is usually delivered via email or a text message, which purports to be from a legitimate source in order to procure personal information. Often such emails do not stand out from other emails users receive from known organisations and contain appropriate logos. Such emails will also contain a demand or a compliance request luring the potential victim to click a link (Cross et al., 2014; Orman, 2013; Parrish, Bailey & Courtney, 2009). Phishing attacks, according to Orman (2013) have certain common characteristics; an email that appears to be from a legitimate business, a website that mimics a legitimate business, a large list of intended victims, an IP address for the website server, malware collecting information from users and may also have malware that tricks users to install it on their computers (Orman, 2013).

Increases in Internet use have meant that the likelihood of phishing attacks is also higher (Hutchings & Hayes, 2008). With the increased sharing of links via social media, users are also increasingly familiar with and therefore less cautious about clicking links

without thinking about the potential dangers, therefore phishing attempts are now also increasingly prevalent on social media platforms (Frauenstein & Flowerday, 2016).

Spear phishing attacks are targeted phishing attacks that are highly personalised, usually designed to look as if they are coming from a person known to the victim. As such, they look more credible and legitimate. Spear phishing attacks are behind some of the very high-profile breeches (e.g. Google). Although more costly and time consuming, they have a much greater rate of success (Parmar, 2012). This suggests that scammers are now designing highly sophisticated and very specific attacks, rather than casting a wide net.

Jagatic, Johnson, Jacobsson and Manczeret (2007) simulated a phishing attack in order to see whether an email coming from a friend rather than from a stranger would influence compliance with a phishing request. Students selected for the study were specifically chosen based on the amount and the quality of the information they shared about themselves online, as this is often how scammers choose their victims. One group of participants received an email purporting to be from a person known to them (i.e. a spoof email), with the goal of redirecting them to a phishing site where they were asked to enter their university details. Another group received an email from a person they did not know but who had a university email from the same institution. They found that phishing emails were more successful when they came from a friend than from a stranger. Emails were also more successful when they purported to come from an opposite gender, with this effect being stronger for men.

More sophisticated phishing attacks may also target specific individuals. Collecting information about the intended victim prior to the attack can often mean that the attack may be more lucrative than just casting a wide net. These types of phishing attacks are known as 'whale phishing', because they target those in high positions in an organisation, such as directors of chief executives (Button et al., 2017; Orman, 2013).

Voice phishing or vishing are telephone scams designed to procure information from a victim. The delivery of a voice phishing email is usually done through Voice Over Internet (VOIP) calling and while this costs more to execute than sending an email, it is also more effective and equally anonymous (Maggi, 2010). Typically, the perpetrator uses stolen personal information about the victim, in order to make them believe the call

is from a legitimate source (e.g. a bank). Further security information is then harvested from the victim, such as the personal identification numbers or other security data (Chang & Lee, 2010). Voice phishing scams are difficult to research due to the fact that there is no physical trace of the phishing attack, such as an email, and reports rely on the victim's account (Maggi, 2010).

With the increasing use of mobile phones and smartphones, fraud is now also perpetrated by smishing, or SMS phishing. Smishing works similarly to ordinary phishing attacks, by asking users to click links embedded in the message, often impersonating legitimate organisations by manipulating the address information (Yan, Eidenbenz & Galli, 2009). Smartphones are particularly vulnerable to phishing attacks, as they run complete operating systems, allowing users to install different applications and to bank via mobile banking. As such, smartphones often contain more sensitive data (Jeon, Kim, Lee &Won, 2011). In addition, smartphones aid different ways of delivery for phishing communication. Reviewing the data on phishing attacks affecting mobile phones, Foozy, Ahmad and Abdollah (2013) identified four different phishing attack strategies; via Bluetooth, SMS, by vishing (i.e. phone phishing) and by mobile web applications. These attacks may result in users exposing their personal information through phishing links or even in the perpetrator gaining partial or full control of the victim's smartphone (Jeon et al., 2011). Frauenstein and Flowerday (2016) argue that the automated behaviour of clicking and sharing links on social media platforms means people are less cautious regarding the information they receive, making phishing attacks more successful.

2.2.5 Lotteries, prize draws and sweepstakes

Fake lotteries, prize draws and sweepstakes follow a similar pattern. Victims are usually sent emails or a letter informing them that they have won a prize or a lottery. In order to claim the prize or access the lottery win, the victims are asked for an administration fee (Button et al., 2009a; Cross et al., 2014).

Lea et al. (2009) conducted interviews with fraud victims examining the scam communication and found that sweepstake scams utilise three main persuasive techniques; perception of authority, quoting large sums of money and stressing the urgency to respond. Communcations often contained barcodes, seals or watermarks making them look official and legitimate and also frequently used the victim's name

throughout. The large prizes are used specifically and often in a cheque form, in order to evoke excitement and urging the victim to respond by a deadline, which is likely to reduce the recipient's motivation to carefully consider the information.

Lottery scams also often utilise several psychological techniques. Similar to sweepstakes and prizes, they offer large prizes in order to entice the victim, stress the urgency to respond and give perception of authority (Button et al., 2009a; Lea et al., 2009). According to Lea et al. (2009), a key distinguishable feature of lottery scams is that they typically do not ask for money, but instead, urge the potential victim to get in contact with an agent to begin the claim. Contact with the scammer is likely to encourage commitment. In one case, the victim contacted the agent only to be told to contact the bank manager, after which the victim was told that there would be a fee to access the win, as she did not reside in the country. After that fee, the victim was contacted again and asked for further fees. Scammers may also contact people that usually participate in lotteries in order to make it more convincing (Button et al., 2009a).

2.2.6 Psychic and clairvoyant scams

Psychic or clairvoyant scams fall under 'sale of bogus products and services' and affect a great number of people. Typically, victims are targeted by mail and offered predictions of the future for a small fee with female and younger populations being more vulnerable to this type of fraud (Button et al., 2009a; Lonsdale, Schweppenstedde, Strang, Stepanek & Stewart, 2016).

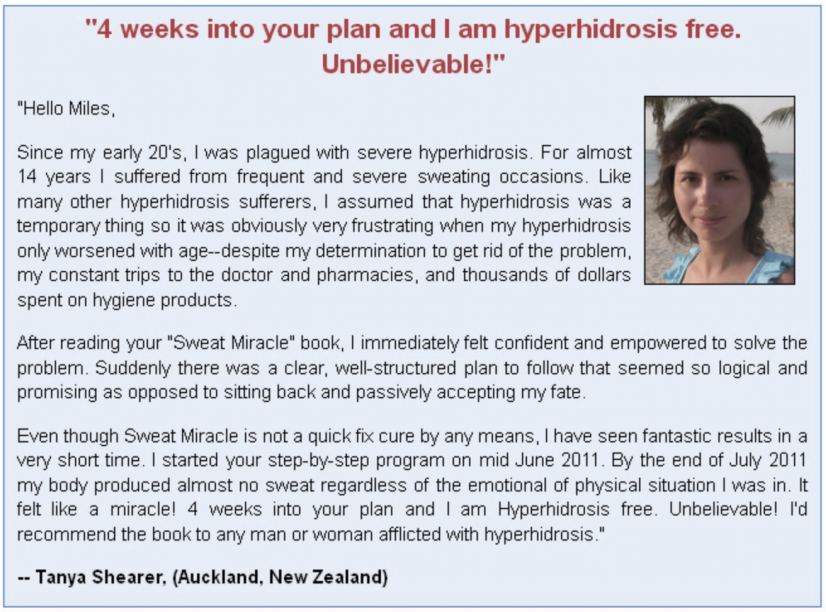
Lea et al. (2009) report that these types of scams use several specific psychological techniques. The communication often mentions deadlines, which may reduce motivation to process information carefully, and contains perceived authority cues, such as mentioned qualifications (e.g. parapsychologist, cosmologist etc.). Sometimes psychic scams evoke fear by mentioning references to danger or a threat and offering protection from the same but can also promise large monetary gains by removing bad luck from the victim. The psychic frequently claims to have a secret knowledge of the victim and to be looking out for them.

The National Centre for Post-Qualifying Social Work and Professional Practice (2016) identified bereaved individuals as particularly vulnerable to this type of scam (also

Olivier, Burls, Fenge & Brown, 2015). Victims of psychic scams can find themselves in a relationship of 'emotional dependence' with the perpetrator (Lea et al., 2009), with some victims blackmailed into paying a fee to protect them or their loved ones from harm (Button, et al., 2009a; Loxton, 2008).

2.2.7 Miracle cures

Miracle cure scams tend to target people with chronic or embarrassing conditions, who are desperate for improvement in their condition. An example of a miracle cure type scam can be seen in Figure 2.2.



"4 weeks into your plan and I am hyperhidrosis free. Unbelievable!"

"Hello Miles,

Since my early 20's, I was plagued with severe hyperhidrosis. For almost 14 years I suffered from frequent and severe sweating occasions. Like many other hyperhidrosis sufferers, I assumed that hyperhidrosis was a temporary thing so it was obviously very frustrating when my hyperhidrosis only worsened with age--despite my determination to get rid of the problem, my constant trips to the doctor and pharmacies, and thousands of dollars spent on hygiene products.

After reading your "Sweat Miracle" book, I immediately felt confident and empowered to solve the problem. Suddenly there was a clear, well-structured plan to follow that seemed so logical and promising as opposed to sitting back and passively accepting my fate.

Even though Sweat Miracle is not a quick fix cure by any means, I have seen fantastic results in a very short time. I started your step-by-step program on mid June 2011. By the end of July 2011 my body produced almost no sweat regardless of the emotional of physical situation I was in. It felt like a miracle! 4 weeks into your plan and I am Hyperhidrosis free. Unbelievable! I'd recommend the book to any man or woman afflicted with hyperhidrosis."

-- Tanya Shearer, (Auckland, New Zealand)

Figure 2.2 Miracle cure scam type correspondence

By analysing the contents of different scams, Lea et al. (2009) found that miracle cure letters most commonly offer cures for obesity, diabetes, impotence, loss of libido, arthritis, baldness and cancer. Lea et al. (2009) suggest these types of scams use social proof cues, such as fake testimonials from other people, to encourage potential victims to purchase the products.

Miracle cure scams may also have a professional and legitimate appearance, but the cures they offer are largely ineffective and could also be dangerous. These types of scams tend to affect women more than men and are rarely reported (Button et al., 2009a).

2.2.8 Business opportunities and investment scams

Another type of a business opportunity scam is a pyramid scheme. Victims are asked to pay a fee to enter a pyramid and by recruiting others, they would earn substantial sums of money. Both these types of scams try to evoke excitement by offering large rewards for little effort although some work from home opportunities keep the amount offered modest, possibly so that it would not arouse suspicion. Scammers often describe themselves as having been in a similar situation to the victim in order to appear similar and often target people who may have difficulty finding a conventional job, either due to disability or family commitments (Lea et al., 2009). Button et al. (2009a) suggests that pyramid or Ponzi schemes tend to target groups of people who work, socialise or attend the same groups and activities together in order to target one victim who would then recruit others, taking advantage of the social influence friends or coworkers may have on one another.

Investment scams are also known as 'boiler room fraud' due to the fact that scammers target victims with high-pressure tactics, often impersonating or cloning legitimate companies in order to add credibility to the scheme. Frauds falling under this category include high-risk investments, property investment schemes (Button et al., 2009a; Kerr et al., 2013) with victims of this type of fraud often having some degree of financial knowledge, making them more confident about their decisions in this area (Lea et al., 2009).

Although the scam examples above are by no means exhaustive; they outline the more frequent fraudulent practices in operation today. However, where there is money to be made there is fraud. To illustrate just how harmful fraud can be, a review by Mohapatra (2012) outlined cases of surrogacy fraud, in which potential surrogates from poorer countries were promised large sums of money to carry a child for a family they had never met, without a surrogacy agreement. After a certain time, they were told the would-be parents had changed their minds and the infants were advertised for adoption. The surrogacy agreements were falsified, leading to problems with legalising the adoption process. This illustrates just how harmful fraud can be and how inventive and callous perpetrators of fraud are becoming.

The interview study in this programme of research (Study 1), considered diverse range of frauds; face-to-face frauds, online frauds using fake websites, pyramid scheme,

investment scam, online auction scam and scams offering jobs and professional training online. The exclusion of the romance scams was made based on the fact that romance scams often include continuous communication over period of months, designed to create deep emotional bonds. Romance scams are, therefore, different from frauds, which require a decision based on the evaluation of the scam offer and were excluded from this programme of research, despite sharing some common elements with other scams (e.g. persuasive techniques such as authority cues, reciprocity etc.).

2.3 Scamming techniques

In a review of different types of Internet fraud and the deceptive techniques each employs, Rusch (1999) found several aspects of social psychology that may explain how certain scams work, such as engaging alternative routes to persuasion, persuasive techniques employed by scammers as well as attitudes and beliefs affecting social interaction. Chang and Chong (2010) analysed the content of different fraudulent e-mails and found that scammers use several coercive techniques to influence potential victims. These included asserting authority and expert status to adopt a position of power over the victim, creating urgency or implying scarcity, sending communications that are very complex in nature and require a great deal of effort to understand, soliciting small commitments to influence bigger commitments at a later time and evoking positive emotions in relation to the scam offer in order to influence the decision-making process. Several of these are common persuasion techniques (Cialdini, 2001) and have been identified by past research (Cukier et al., 2007; Langenderfer & Shimp, 2001; Lea et al., 2009; Rusch, 1999; Zuckoff, 2005). These techniques will now be discussed.

2.3.1 Evoking visceral influence

Using data on consumer fraud and behaviour, conducted by an American Organization for Retired People's interests and by surveying the employees of the Better Business Bureau (BBB), a non-profit organization that promotes ethical business conducts, Langenderfer and Shimp (2001) proposed a theoretical model of scamming vulnerability that outlined visceral influence as a factor that contributes to scam vulnerability, by directing the victim's attention away from rational thinking (Figure 2.3).

Lowestein (1996) describes visceral influences as primal drive states, such as fear, hunger, greed, sexual desires etc. (also Ariely & Loewenstein, 2006). A person under visceral influence is likely to divert their attention from careful information processing towards the attainment of an object or an activity that would satisfy the visceral need (e.g. a hungry person tends to think about food). For example, positive emotions evoked by an attractive scam offer lead to a lowered risk perception and increase the likelihood of impulsive behaviour (Slovic & Peters, 2006). Scams are frequently designed to evoke visceral influences to compromise careful thinking (Langenderfer & Shimp, 2001; Rusch, 1999). Due to the fact that visceral influence tends to be temporary, many scams also emphasise quick decision making by imposing time limits to scam offers (Langenderfer & Shimp, 2001).

Visceral influence can be triggered by the thought of high prizes (e.g. a lottery win) or the promise of a cure that would alleviate pain (Lea et al., 2009). Visceral influence is greater when the scam reward appears close in time and space, and is vivid. Vividness can be manipulated by telling the potential victim someone similar to them has also received the scam reward and has profited from it (Langenderfer & Shimp, 2001).

Many frauds perpetrated online are designed to trigger strong emotional responses in order to detract from rational thinking (Cukier et al., 2007). For example, phishing emails suggesting the account of a victim has been compromised to evoke fear or panic, making the victim more likely to use the links provided in the email to correct this.

2.3.2 Liking and similarity

Scammers are often skilled at appearing likeable and pretend to like their victims in order to persuade them; as people like those who like them (Lea et al., 2009). Giving compliments and having frequent contact with a victim is also thought to facilitate liking. Since people are thought to like those similar to them in some way, scammers may dress or act similar to the potential victim or pretend to have similar interests, problems or background (Cialdini, 2001). For example, in her interview study with romance fraud victims, Whitty (2013) found that scammers often told their victims that they had the same interests as them or liked the same things and this similarity enhanced the feeling of closeness. Analysing scam communication, Lea et al. (2009) found that some types of scams use similarity to influence the potential victim, by using phrases such as 'I was just like you' or 'I was in your situation'.

Research also found that similarity could reduce the perceived threat. Silvia (2005) conducted an experiment in which participants were given an essay to read on a certain topic. The essay was manipulated to either include threatening elements (e.g. sentences strongly expressing opposing attitudes) or exclude threatening elements. Participants were asked to rate certain values (e.g. accomplishment, true friendship, justice) on how important they were to them and these answers were used as a similarity manipulation for the essays. Some participants received an essay with a profile of the author, which was based on their own ratings of certain values, while other participants received the same essay but the profile of the author was dissimilar to them. They then completed the questionnaire measuring agreement with the author of the essay, opinions on whether the author was trying to persuade them or stop them from making up their mind. The study found that when similarity between the participants and the author of the essay was low, participants did not agree with essays containing the threatening elements as much as they agreed with essays containing no threats. But when the similarity was high between the participants and the author of the essay, participants agreed with the author of the essay, regardless of whether it contained the threatening elements or not. Additionally, when similarity was high, the communication was perceived as less coercive than when the similarity was low. Similarity, Silvia (2005) argues, can reduce the perceived threat as well as enhance liking, which can influence compliance by minimising the difference in opinions.

2.3.3 Evoking social norms

People tend to prize several socially benevolent characteristics, such as being a good citizen, being charitable, helpful or kind. These attributes are often exploited by scammers who may pretend they are vulnerable or in need of help (Lea et al., 2009; Titus & Gover, 2001; Witty, 2013).

Another socially desirable behaviour is reciprocating a favour. Scammers may exploit this by giving a small gift to a victim in order to facilitate reciprocation later. For example, Whitty (2013) found that in some cases of romance fraud, the perpetrator would send the victim a gift, such as flowers or other love tokens, and this act would facilitate compliance with a subsequent request for money. One victim reported that this gesture even convinced her friend that the scammer was a genuine person, and this was the moment that she started sending funds.

Another way reciprocation can be exploited is by making an extreme request, likely to be immediately rejected, in order to make a smaller request, which then appears as a concession and is more likely to be accepted (Cialdini, 2001). In the study by Benton, Kelley and Liebling (1972), participants were told to decide, with an opponent, how the money they were given should be divided between them. If a decision could not be reached, the money would be withheld. The opponent (research assistant) would either make a demand for a large sum of money and refuse to lower the amount, request a low sum of money and maintain this through negotiations or make a demand for a large sum and when rejected, slowly reduce the demanded amount. The study found that participants made more generous offers when their opponent first demanded large sums of money and then reduced their demands than compared to the other two conditions. Participants also reported feeling more satisfied with the outcome in this condition.

2.3.4 Authority

Scams often purport to be from someone in a position of authority, such as a solicitor, doctor, police officer or a bank official, in order to facilitate compliance. People tend to trust and obey authoritative figures, as this constitutes correct conduct, and are therefore more likely to comply (Cialdini, 2001; Lea et al., 2009; Modic & Lea, 2013; Whitty, 2013; Whitty & Buchanan, 2012b).

Examining different scam communications, Lea et al. (2009) found that scam offers often purport to be from someone in a position of authority (e.g. in a position to facilitate the offer). Conducting interviews with romance fraud victims, Whitty and Buchanan (2012a) found that in the later stages of a romance scam, a victim is often told the romantic partner is in trouble and a third person is introduced to the scam. This person is often in a position of authority; a doctor, a police officer or a lawyer. They argue that this technique is deliberate as people are more likely to comply with authority figures.

Workman (2008) investigated security breaches in a large organisation. Employees were given questionnaire items based on previous research, measuring commitments (Allen & Meyer, 1990), reactance/resistance (i.e. motivational reaction to rules, offers or people, perceived to threaten behavioural freedoms) and obedience to authority (Massi Lindsey, 2005; Weatherly, Miller & McDonald, 1999) and trust (Gendall, 2005). In addition, Workman (2008) conducted a field study over a period of 6 months,

consisting of objective observations, where participants were not aware what was being studied. Participants were sent previously successful phishing emails, which were followed up by phone calls pretending to be from internal employees or trading partners, utility companies and financial institutions in order to gain confidential information from participants using persuasive techniques. They found that obedience to authority, high normative commitment (e.g. reciprocity) and trust lead to greater vulnerability to social engineering attacks such as phishing or phone phishing.

These findings are consistent with findings by Fischer, Lea and Evans (2013), who analysed the data from a series of fraud research studies conducted by Lea et al. (2009). Fischer et al. (2013) found that scam victims were more influenced by fake signs of authority, often used by scammers to enhance compliance. Using interviews transcripts to identify words most frequently mentioned, Fischer et al. (2013) found authority as one of the words frequently mentioned by victims when recounting their experience. Additionally, Fischer et al. (2013) simulated a postal scam, followed up by a questionnaire asking for reaction to the same scam. They found that trust associated with the scam offer varied according to whether symbols of authority were present. However, this was not confirmed in the consequent study, and the authors suggested that this may be due to the complex ways in which content factors interact in order to make a scam offer attractive. However, it could be argued that these differences may also be attributed to individual differences. For example, in their study, Modic and Lea (2013) developed a measure of susceptibility to persuasion, which was administered to participants who were also asked to evaluate real life situations that could potentially be scams. Participants were asked if they thought it was likely that each scenario was a scam and whether they had ever found themselves in, responded to, or lost money in such a situation. They found that authority (e.g. being influenced by authority figures) predicted whether someone is likely to respond to fraud offers. Therefore, personal attributes may also play a role in how affective scam content factors are in persuading one to respond or comply with fraudulent offers.

2.3.5 Scarcity and urgency

When something is scarce or not easily available, people will assign more value to it. Limiting the quantity or limiting the duration of an offer can simulate scarcity. When something desired is not easily available, it becomes even more desirable. Scarcity also makes things appear more valuable by skewing the perception of quality (Cialdini,

2001). For example, Kramer and Carroll (2009) conducted several experiments, which explored out of stock options on purchase intention. In one of their studies, they asked participants to imagine they are at a store deciding to purchase a mobile phone that was described as being an average size with an average battery life. Some participants were told other phones were out of stock (e.g. larger phone with longer battery life or smaller phone with shorter battery life) while the control group was not given this information. Participants then had to rate the likelihood of purchasing the phone. The study found that when participants were told other phones were out of stock, they were significantly more likely to purchase the average phone. Kramer and Carroll (2009) suggest this is due to scarcity cues.

Scammers are often thought to emphasize the uniqueness of the scam offer and urge the potential victim to make an instant decision in order to avoid losing the opportunity. Stajano and Wilson (2010) researched different scams in order to examine techniques used by scammers, as well as behavioural patterns of fraud victims. They found that scammers often emphasise that the offer is a 'one time offer' and the potential victim needs to act quickly. This approach is also used in some phishing scams, such as those that urge the victim to urgently confirm their details or their account access will be blocked. However, research by Fischer et al. (2013) found that scarcity cues in scam correspondence might have the opposite effect, making the potential victim more suspicious. This suggests that while some people may be influenced by these scamming techniques, others are able to recognise them and apply caution.

2.3.6 Social proof and social influence

People shape their beliefs and behaviour by looking at how others behave and what they believe, therefore scam offers that have bogus testimonials or the backing of other people tend to be more successful (Cialdini, 2001; Stajano & Wilson, 2011).

Lea et al. (2009) found that social proof can be a feature of some business opportunity scams as they often contain fake testimonials of people who have previously benefitted from the opportunity. Stajano and Wilson (2011) found that social proof or what they call 'herd principle' is often used as scamming techniques as people let their guard down when they see others taking risks. For example, in auction scams, shills, or fake bidders may bid on items for sale and leave the feedback for the seller. This bogus feedback

will inspire confidence in others who want to buy from the same seller. Scammers also frequently set up fake aliases on social media or other online communications platforms, in order to convince potential victims that there are others who share the same opinion.

Research by Modic and Lea (2013) also found that those who scored more highly on a measure of social influence (i.e. being influenced by their peers or social circle) were more likely to respond to fraud offers. They suggested that scammers might exploit this by pretending to have a close relationship with potential victims in order to prompt compliance.

However, in some cases, scams may encourage avoidance of social influence, possibly to stop the victim from discussing it with others and becoming suspicious. Lea et al. (2009) found that lottery scams frequently urge the potential victim to keep the win confidential by stating that the leaked information may result in double claims by others, and this would make the win void.

2.3.7 Commitment and consistency

In his review of known persuasion techniques, Cialdini (2001) suggests that personal consistency is a desired and culturally valued personality trait, referring to one's personal beliefs being in accordance (i.e. consistent) with one's behaviour. People appreciate when theirs and others' beliefs and behaviours are consistent, therefore a person who exhibits inconsistent beliefs may be viewed as two-faced or confused. Scammers exploit this. For example, once a scammer succeeds in persuading the potential victim to respond, it makes it easier to also get them to comply with future requests (Cialdini & Goldstein, 2004). Scammers often request a response without asking for money first for that reason. Lea et al. (2009) found that lottery scams often ask potential victims to get in touch with various different people so that the lottery win can be processed. This fosters commitment. Fischer et al. (2013) examined a large body of different scam communications and found that scammers often asked for small commitments from the victim, such as returning a letter or sending a small fee. These small commitments make it more likely that the victim will cooperate further in the future. Additionally, Modic and Lea (2013) found that consistency (i.e. the need to honour previous commitments) predicted responding to scam offers.

2.3.8 Dishonesty and distraction principles

By analysing different scams and scamming techniques, Stajano and Wilson (2011) found that some scams are based on declared dishonesty and distraction principles. Scammers sometimes openly tell their victim that what they are getting involved in is illegal and that this is the reason the victim is getting a 'good deal'. For example, Nigerian or 419 scams sometimes use this technique (e.g. money laundering) and victims, once defrauded, may feel they have no recourse because they did something illegal. Additionally, scammers are good at distracting victims from thinking about negative issues. For example, distraction can be applied by emphasizing the size of the reward in order to detract from the warning signs.

Successful deception relies on rational beliefs people have about the world and the way they respond to it, therefore a deceiver needs to know what the victim perceives as 'regular' in order to act accordingly. This requires extensive knowledge that incorporates psychology, cultural conventions and regular life patterns of the victim (Mitchell, 1996). As such, scams can be extremely sophisticated events. Identifying techniques employed by scammers offers an insight into the scam process, however this process also depends on other components, such as individual differences, which may increase vulnerability to fraud.

2.4 Theories and models of scam vulnerability

The literature reviewed above shows how fraud techniques, social mechanisms and other situational factors have an impact on scam victimisation, however a different way of approaching the phenomenon is at the individual level. In addition to different scamming and social engineering techniques frequently used to encourage scam compliance, different theories and psychological models have been proposed to assist the understanding of how different factors combine to influence compliance with fraudulent offers.

2.4.1 Errors of judgment

Research by Lea et al. (2009), which consisted of four large-scale studies, including extended interviews with victims of scams and the text mining of scam communication materials, identified different factors involved in errors of judgment connected to scams.

These errors are separated into two groups; motivational and cognitive (Table 2.3).

Table 2.3.
Cognitive and motivational factors involved in errors of judgment by Lea, Fischer and Evans (2009)

Motivational Factors		**Cognitive Factors**	
Factor	Description	Factor	Description
Visceral influence	Basic human desires and needs (e.g. greed, fear etc.)	Reduced cognitive abilities	Cognitive abilities are necessary for decision making and to distinguish legitimate offers from scams
Reduced motivation for information processing	Triggered by scam communication such as scarcity of the offer or visceral influence, but can be a result of cognitive impairment	Positive illusions	Tendency to see oneself in a positive light and overestimate one's abilities
Preference for confirmation	Tendency to seek information that confirms one's preferences	Background knowledge and overconfidence	Background knowledge can lead to overconfidence in one's decisions
Lack of self-control	Inability to regulate emotional responses	Norm activation	Scams often target specific social norms, such as helping others, being polite etc.
Mood regulation and phantom fixation	Attempt to control mental states, such as trying to avoid a negative mood by shopping	False consensus	Overestimating the reliability and validity of an offer because it has a backing of other people
Sensation seeking	Emotional effects which elicit excitement and arousal, associated with risk taking	Authority	Tendency to obey authority
Liking and similarity	Tendency to like those that like us and are similar to us	Social proof	Tendency to look to others to define our reality
Reciprocation	Basic tendency to want to reciprocate the favour	Altercasting	Scammers often place their victims in complimentary roles (e.g. a friend)
Commitment and consistency	Exploiting people's desires for consistency in the behaviour, theirs and other's by initiating communication before asking for money		

For example, scams evoke visceral influence by offering high rewards for little effort on the victim's part, while the authority is established by purporting the offer is backed by someone in a position of authority (e.g. bank official, solicitor, director etc.). These techniques are used in order to detract from careful information processing, to evoke errors in judgments in order to facilitate scam compliance.

The following two studies by Lea et al. (2009) compared susceptibility of these errors of judgment in victims of scams and those that have not been scammed in the past. The first study involved constructing a questionnaire consisting of statements that identified different errors of judgment connected to scam vulnerability and asking participants to indicate their feelings about the scam offers received in the past in connection with these errors. Participants were separated into two groups; those that have never been a victim of a scam and those that were scammed in the past. The findings indicated that the two groups differed in their tendency to commit judgment errors, with those classed as non-victims showing no or very little agreement with the statements, whereas victims and near victims report medium agreement with the statements. They postulated that victims have a general vulnerability to persuasion, not just a specific weakness towards the type of scam offer they responded to.

The following study was a simulated scam experiment, in which a scam letter, designed to include the content cues affecting errors in judgment (e.g. high prize, official looking letter, urgency cues etc.) was sent to unsuspecting participants. Differences emerged between those who report previously responding to scams and those who do not, with previous responders more likely to respond again and showing less dislike of the scam situation. Lea et al. (2009) suggest this means that certain people may be particularly vulnerable to repeat victimisation.

Lea et al. (2009) studies explain how certain scamming techniques work to affect people's judgments when evaluating fraudulent communication. The studies also demonstrated that individual vulnerability varies between people, with some people being more likely to respond to fraudulent offers, however, the study did not measure personal attributes that may underlie the likelihood of responding when simulating a fraudulent situation.

2.4.2 Model of scamming vulnerability

The theoretical model of scamming vulnerability by Langenderfer and Shimp (2001) was based on the large-scale research conducted with elderly victims of fraud by the American Association of Retired People and their own survey of scam experts from Better Business Bureau (BBB), a non-profit organisation, promoting ethical business conduct for elderly people. By evaluating the available data, several distinguishing characteristics that distinguished fraud victims from non-victims emerged; trusting nature, gullibility, being fantasy prone, advanced age, greed and social isolation.

Langenderfer and Shimp (2001) posit that differences in the attention people pay to fraudulent messages can be considered in the context of Petty and Cacioppo's (1986) Elaboration Likelihood Model (ELM) of persuasion, which has two routes of information processing; peripheral and central (Figure 2.7). The peripheral route utilises little elaboration or evaluation of message content and relies on persuasive cues such as the attractiveness of the scam offer, while the central route concentrates on the arguments provided. Langenderfer and Shimp (2001) suggest that when the elaboration likelihood is high but visceral influence is low, attention is directed at the arguments in the message rather than the rewards, which would help spot deception. When the elaboration likelihood is high and the degree of visceral influence is also high, attention is directed at the reward arguments and away from cues that may help detect deception. The authors also argue that visceral influence is greater when the prize seems close in time and space (proximity) and when it can be imagined easily (vividness), and this can be manipulated by telling the victim about other people, similar to them, who have enjoyed the same opportunity. Langenderfer and Shimp's (2001) theoretical Model of Scamming Vulnerability explains how the attention is directed under high and low visceral influence and can be found in Figure 2.3.

Under high visceral influence, the focus is on the scam reward (e.g. the size of the prize), rather than on scam cues, which may alert to potential danger. In this state, self-control acts as a moderator of scamming vulnerability. In situations where the degree of visceral influence is low and the attention is on the scam cues, there are still factors that can contribute to vulnerability to scams. These factors are assumed to include social isolation, cognitive impairment, gullibility and consumer susceptibility to interpersonal influence. Moderators of scam vulnerability, when the degree of visceral influence is low are scepticism and scam knowledge.

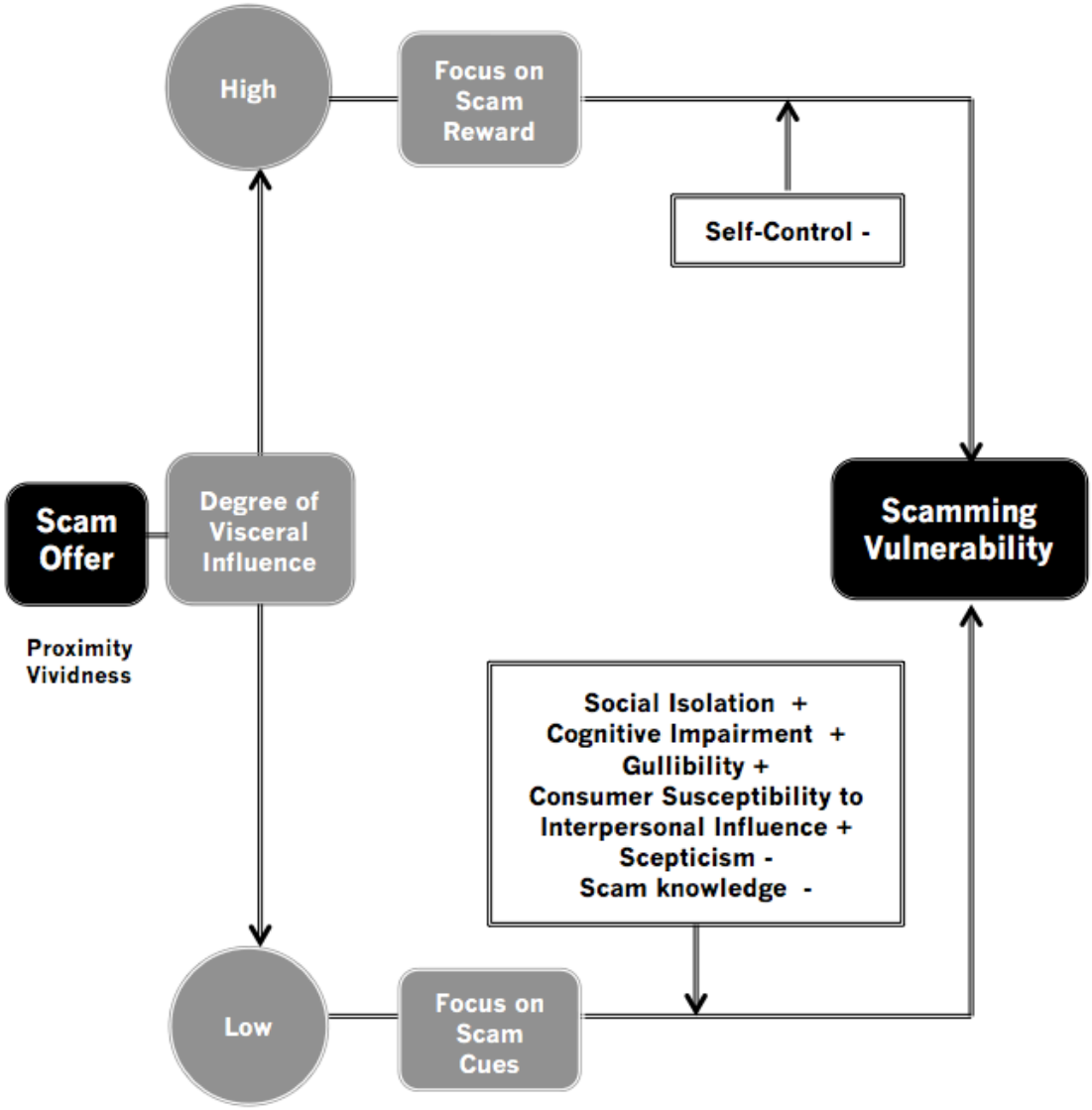


Figure 2.3. Langenderfer and Shimp (2001) Model of Scamming Vulnerability and its moderators under high and low visceral influence

Although Langenderfer and Shimp (2001) theoretical model offers a detailed explanation of scamming vulnerability under low and high visceral influence and in presence of certain individual attributes, it has not been empirically tested. Additionally, the data used for the development of this theoretical framework was based on the consumer fraud affecting elderly consumers. Given the fact that the elderly individuals may be more vulnerable to scams due to diminishing cognitive functions (Langenderfer & Shimp, 2001) and may be more likely to have a preference for positive over negative information (Löckenhoff & Carstensen, 2007; Reed & Carstensen, 2012), the findings may not be generalizable across different scam contexts and age groups.

2.4.3 Models of gullible and foolish action

In his review of foolish action, Greenspan (2008) described 'foolish action' as a human behaviour found in everyone, which has a high likelihood of backfiring at times. Greenspan (2008) further proposed theoretical Model of Foolish Action, divided into socially and practically foolish actions. Practically foolish actions usually result in physical danger (i.e. smoking at the petrol station) and socially foolish actions have interpersonal consequences and is sub-divided into induced and non-induced. Induced foolish action happens in the presence of manipulation by person(s), usually on the basis of false information against one's best interests and this induced foolish action manifesting itself as "gullibility" (Greenspan, 2008). The Model of Foolish Action is found in Figure 2.4.

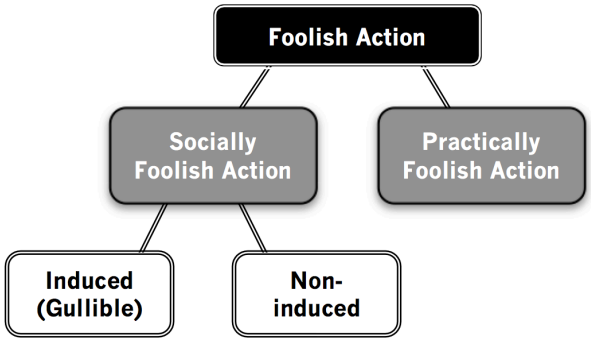


Figure 2.4 The Model of Foolish Action proposed by Greenspan (2008)

Furthermore, Greenspan, Switzky and Woods (2011) posit that common sense relates to a sound judgment or awareness of obvious social or practical risk. It is intuitive and not dependent on special knowledge and cannot be mistaken for intelligence quotient (IQ).

Social risk refers to danger of harm from other people or a society and practical risk refers to physical harm (e.g. from objects). They suggest that 'foolishness' is a frequent term that describes unawareness of obvious risk, whereas common sense is awareness of obvious risk. Although their theory concentrates on populations with intellectual disabilities, the idea of common sense may also be applied to general population.

In his review on gullibility, Greenspan (2009) suggests that gullibility is something that almost anyone can relate to, yet not much exists on this topic in scholarly literature. Defining gullibility as "an unusual tendency toward being duped or taken advantage of' (p.2), Greenspan (2009) argues that gullibility and credulity are different in that

gullibility usually results in some type of action. He proposed an explanatory model of gullible action, consisting of four components; situation, cognition, personality and state (Figure 2.5). Any combination of these components or even one strong component can influence people to engage in acts that are against their best interests. An identical model, citing the same four components as the model of Gullible action, is proposed by Greenspan (2008) as a model of Foolish action. This may suggest that foolish action and gullible action may share the same components.

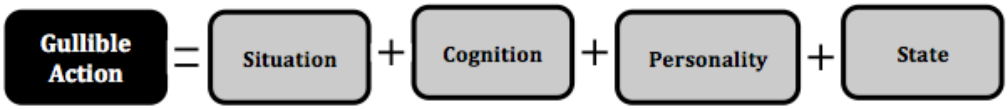


Figure 2.5 The Model of Gullible Action proposed by Greenspan (2009)

Social situation (e.g. persuasiveness of the scammer or others recommending him), cognitive processes (being bad at reading people or naïve about the offer), personality (victim being too trusting or too agreeable) and affect or state (i.e. being infatuated with the scammer) may influence gullible action (Greenspan, 2009).

Referring to cognitive processes in his model, Greenspan (2009) suggests that 'intelligence' is not always connected to gullible action. Gullibility does not reflect an inability to think, but it can be a product of lazy thinking. Highly intelligent people may also be lacking social and practical intelligence, making them unable to recognise deceptive cues.

Greenspan (2009) also suggests that rushing decisions or making decisions when one is under the influence of strong emotions is more likely to result in gullible action. Thinking without the influence of the strong emotion (i.e. cold cognition) is more likely to be rational than thinking under the influence of the strong emotion (i.e. hot cognition). In order to avoid being gullible, one must understand the limitations of one's knowledge and when in misleading or dangerous situations, be prepared to postpone decisions. The Model of Gullible Action, therefore, offers support for Langenderfer and Shimp (2001) Model of Scamming Vulnerability, in which information processing under the visceral influence leads to hot cognition (i.e. under the influence of emotion) and the prospect of missing the scam cues. Although the model

of Gullible action has not been empirically tested and Greenspan (2008) does not specify how the model could be practically applied, its components could be useful in explaining factors that interact to encourage compliance with fraudulent offers.

2.4.4 Phishing susceptibility framework

Parrish, Bailey and Courtney (2009) proposed a phishing susceptibility framework, using the Big-Five personality factors, suggesting that scams target certain human traits and that individuals who are high in those traits may be more susceptible. As well as personality traits, their framework also outlines personal (e.g. gender, age, culture) and experiential factors (past events and experience that shape individual's personality). They argue that each of these factors is implicated in an individual's vulnerability to phishing attacks and that each factor may be implicated in the development of another factor. For example, personal factors such as age and culture, may influence an individual's experience and both, personal and experiential factors may play a role in personality development. The framework proposed by Parrish et al. (2009) can be found in Figure 2.6.

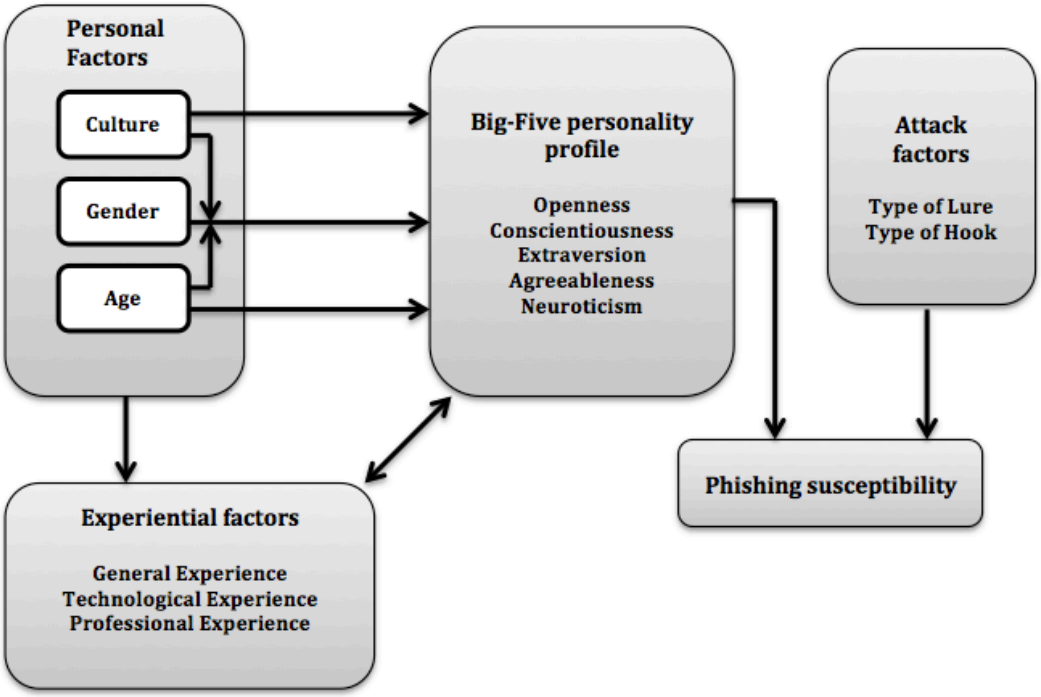


Figure 2.6. Phishing Susceptibility Framework by Parrish, Bailey and Courtney (2009)

Experiential factors include general experience, which can be positive or negative, technological experience (e.g. internet usage or experience) and professional experience, such as a career or academic experience. Attack factors include the lure (e.g. security upgrade, financial incentive, false account updates etc.) and the hook (e.g. link to a website or a reply to email, text message etc.) Phishing susceptibility includes the likelihood to respond and the time it takes to respond.

Personal factors, such as culture, gender and age influence factors of the Big-Five personality profile, as well as experiential factors. Culture and age may, in some cases have moderating effects on gender, while the Big-Five personality factors have a direct effect on experiential factors and vice versa. They also directly influence phishing susceptibility. Phishing susceptibility is further influenced by factors pertaining to the attack, such as the type of lure and hook they contain.

Looking at the Big-Five personality profile factors, Parrish et al. (2009) suggest that agreeableness may be associated with susceptibility to phishing attacks due to the trust dimension it contains, while extraversion is implicated in susceptibility due to the fact that extraverts may be more likely to share information with others. General openness to experience, may also be implicated in susceptibility to phishing attacks. However, conscientiousness, they argued, may prevent susceptibility to phishing if a person has received some security guidelines, as they are more likely to follow those guidelines. Neuroticism, too, may prevent susceptibility to phishing as those high on neuroticism may be less eager to share their details online and even have less online exposure than those that are lower on neuroticism.

Although focused on phishing scams, their theory leads to a broader hypothesis which might be applied to all types of scams, that there are certain individual difference variables that may predict which people may be more vulnerable to fraud. For example, research by Modic and Lea (2012) looked at the personality traits that may influence scam compliance. In their study participants completed scales measuring the Big-Five personality traits, self-control and impulsivity. Participants also received life scenarios that could be potential scam situations and asked to evaluate how likely is it that a scenario is a scam and how likely it is that people would respond favourably to it. Participants were also asked if they experienced, responded and lost money to such a scenario. Contrary to Parrish et al. (2009) prediction that extraverts would be more

vulnerable to phishing attacks, Modic and Lea (2012) found that extraversion was a good predictor of increased scam response, but in the opposite direction, with more introverted individuals being more likely to respond to scams. They suggested that this might be due to the fact that they prefer impersonal contact, such as communicating online, which makes it difficult to tell whether a person is trustworthy. It could also be that they have fewer friends and family members they regularly communicate with. Modic and Lea (2012) also found agreeableness to be a predictor of responding to a scam, suggesting this is due to the fact that agreeable individuals tend to be considerate and friendly, therefore, they may believe others are too.

2.5 Individual differences and fraud vulnerability

Receiving fraudulent offers does not automatically mean one will become a victim of a scam and identifying what makes one vulnerable to fraud is not always easy. Research indicates that some fraud victims are highly educated, fully functioning adults and seem to be unlikely victims (Cacciottolo and Rees, 2017; Lea et al., 2009; Zuckoff, 2005), so what are the factors influencing compliance with fraudulent offers?

2.5.1 Self-control, premeditation and impulsivity

Inability to control one's impulses has been found to compromise decision making (Bayard, Raffard & Gely-Nargeot, 2011). It has also been found to influence likelihood of fraud victimisation. Lack of self-control has also been found to increase the risk of criminal victimisation in general (Schreck 1999; Schreck, Stewart & Fisher, 2006). A meta-analysis of 66 studies on crime victimisation, by Pratt, Turanovic, Fox and Wright (2014) found that self-control is a consistent predictor of victimisation and is significantly stronger when victimisation takes place without a contact, such as online. Self-control has also been implicated in fraud victimisation. Some authors have suggested that scam victims lack emotional control when it comes to their interpretation and engagement with scam offers (Lea et al., 2009). For example, Langenderfer and Shimp (2001) interviewed experts working in an organisation offering consumer protection to the elderly and found that scam vulnerability is often greater in those who cannot control their emotional responses. This is consistent with research based on telephone surveys with those over the age of sixty by Holtfreter, Reisig, Pratt and Holtfreter (2015). They found that elderly people who have lower levels of self-control

were more likely to make a purchase from an unknown vendor, after receiving an unsolicited email. Making such purchases can be risky and leave them open to identity theft. However, Holtfreter et al. (2015) noted that their study used a two-item measure of self-control and further studies, with valid measures of self-control are needed.

In their study, Holtfreter, Reisig, Piquero and Piquero (2010) gave student participants hypothetical offending and victimisation scenarios based on some methods scammers use to target potential victims, as well as a measure of self-control. After each scenario, students were also asked to indicate the likelihood of engaging in such behaviour. They found low self-control to be positively related to fraud victimisation, suggesting that those with lower levels of self-control were more likely to report they would engage in behaviours that lead to fraud victimisation. This is consistent with Modic and Lea (2012) who found that premeditation (part of an impulsivity scale), or the ability to foresee future consequences, was a good predictor of whether someone is likely to respond to fraudulent offers.

Holtfreter, Reisig and Pratt (2008) conducted phone interviews in order to explore remote purchases and fraud victimisation and fraud targeting. Participants were also given items measuring preference for risky behaviours and immediate gratification, which would pinpoint low self-control. They found that those who made more remote purchases (e.g. purchases online) were more likely to be targeted by fraudulent offers and also more likely to have been victims of fraud. Although lack of self-control did not predict being targeted by fraudulent offers, it did predict fraud victimisation and Holtfreter et al. (2008) suggest this may be due to the fact that those low in self-control are likely to be impulsive and more likely to act when presented with fraudulent offers.

Impulsivity has also been found to affect decision-making. In a study by Frederick (2005), participants received the Cognitive Reflection Test (CRT) measure (a measure that tests reliance on logic versus intuition), measures of their decision-making characteristics and self-reported measures of impulsivity. The study found that those who achieved higher scores on CRT measures were more patient (i.e. less impulsive) and less likely to opt for paying more money to get the desired items delivered quicker (time preference). They were also less likely to take risks in the gambling task.

2.5.2 Background and scam knowledge

People lacking general interest in current events may be more vulnerable to fraudulent offers, as they may not be aware of current scams or related developments (Titus & Gover, 2001). Langenderfer and Shimp (2001) found that lack of scam knowledge or knowledge of an area relevant to a particular scam (i.e. investments), may be implicated in scam vulnerability, however Lea et al. (2009) suggest that background knowledge enhances vulnerability by leading to less caution. For example, investment scams often affect those that have background knowledge in the same area of expertise.

2.5.3 Information processing

Differences in the attention people pay to fraudulent messages can be considered in the context of Petty and Cacioppo's (1986) Elaboration Likelihood Model (ELM) of persuasion (Figure 2.7).

When a persuasive message is received, one of the two routes will be chosen depending on the motivation and the ability to process the relevant information. Using the peripheral route, one is likely to concentrate on superficial cues, such as how attractive the offer is, instead of seeking evidence to support the claims in the persuasive message. The central route is likely to concentrate on the message arguments and lead to an attitude change based on the argument quality. Cacioppo and Petty (1982) argued that individuals low in the psychological construct, 'need for cognition' (who do not enjoy effortful cognitive activities) tend to process information via the peripheral route, unlike those with high need for cognition, who rely less on peripheral cues and process information by exerting greater cognitive effort.

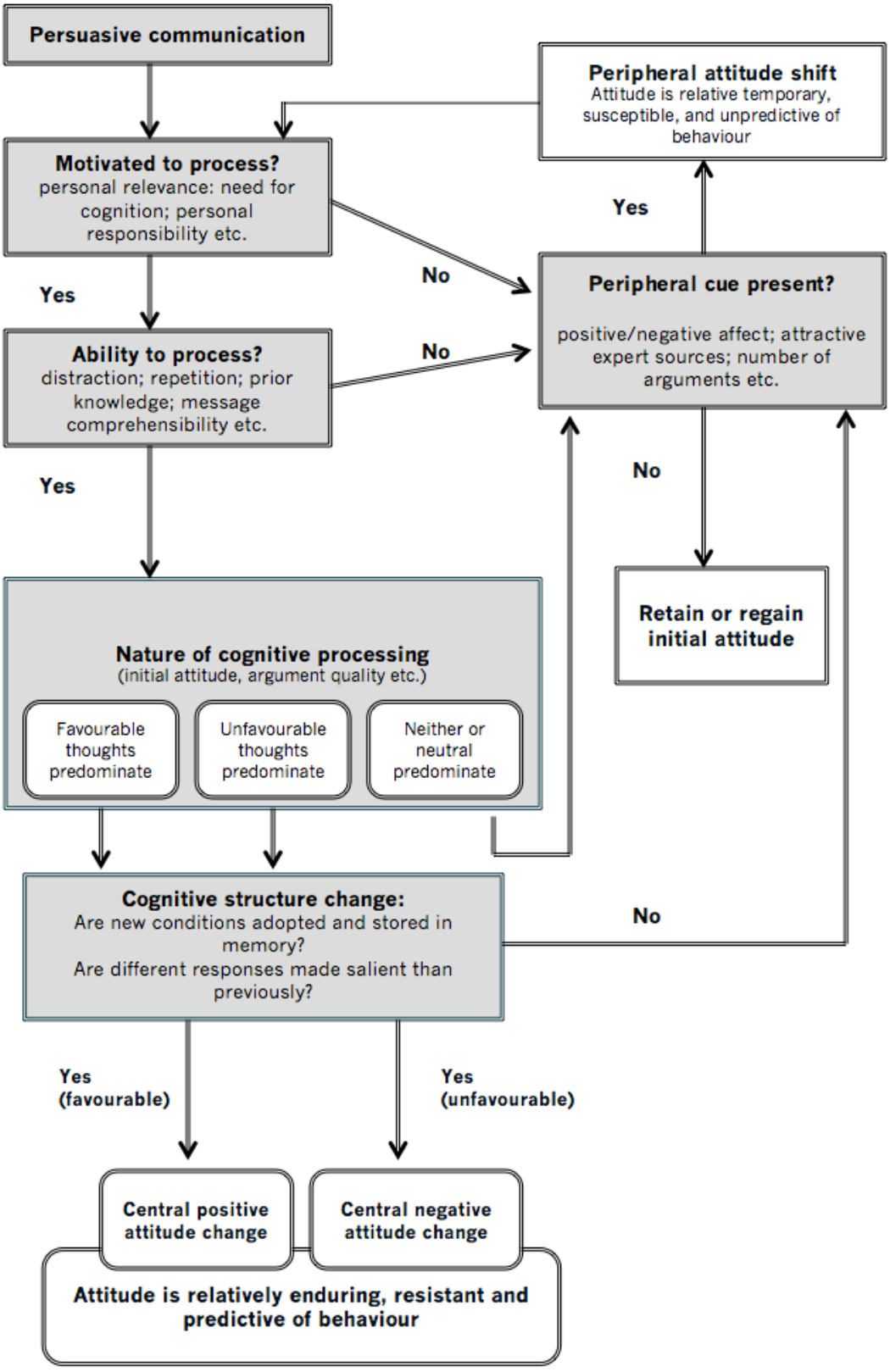


Figure 2.7 Petty and Cacioppo's (1986) Elaboration Likelihood Model of persuasion

In the study by Cacioppo, Petty, Kao and Rodriguez (1986), participants were given a Need for Cognition measure (Cacioppo et al., 1984) and were asked to listen to a recorded message about tuition fees. The arguments in the message were purposely made weak or strong and participants were asked specific questions about argument quality after they listened to the message, as well as being asked their opinion on the subject of tuition fees. They were also asked to recall their thoughts while they were listening to the message and to write down as many arguments they remember from the message they heard. Participants were also asked to report how much effort they put into evaluating the message. The study found that individuals low in 'need for cognition' were less discriminating when evaluating weak and strong messages, were less affected by argument quality and recalled fewer arguments when asked. They also reported expending less effort evaluating arguments than those high in need for cognition.

Research by Kaufman, Stasson and Hart (1999) found that people high in need for cognition are less likely to be influenced by source credibility. In their study, participants were given an article to read that varied in argument strength. The arguments were either weak (ambiguous and lacking in facts and references to credible sources) or strong (factual statements with credible references and written more eloquently). Participants were also told that the article came from reputable newspaper (credible source) or a low credibility magazine. The study found that those low in Need for Cognition rated weak arguments more highly when they came from a reputable source. However, they paid more attention to argument strength when they were made to believe the article came from a non-reputable (low credibility) source. Kaufman et al. (1999) suggest this means that untrustworthy sources may motivate greater information processing among those low in need for cognition. Scammers often impersonate legitimate sources, which could mean that those with lower need for cognition might be more likely to accept fraudulent offers that look authentic rather than process the information relevant to the offer. This interpretation is supported by the analysis of phishing attempts, which mimic bank communications, by Blythe, Petrie and Clark (2011). The authors found that blind participants were better at spotting phishing emails since they were not visually primed by familiar company logos. Instead their computer reading software read the message, alerting them to warning signs, such as phrasing or spelling mistakes, which made them suspect the correspondence may not be genuine.

Other research, however, has suggested that scam victims report analysing scam offers more thoroughly than non-victims and that this may be making them vulnerable. While some people discard unsolicited scam offers without reading them, reading the scam offer may elicit curiosity to respond (Lea et al., 2009).

Information processing may also be influenced by individual characteristics. For example, Haddock, Maio and Huskinson (2008) found that when the content of a message is matched to an individual's personality, it is found to be more persuasive. In their study, participants were given messages about a new drink to evaluate, which were either cognition-based (message describing a drink as pleasant) or affect-based (message citing facts about the drink). Those high in need for cognition found a cognition-based message more persuasive, while those high in need for affect found an affect-based message more persuasive. This suggests that scam offers may be perceived as more attractive if they contain cues that accommodate certain individual attributes.

2.5.4 Assessing risks and sensation seeking

It has been suggested that some fraud victims see scam offers as a long odds gamble. They recognise there may be risk involved but decide to go ahead with it hoping it will pay out. If the promised reward is sufficiently large, the offer may seem worth the risk (Lea et al., 2009). Olivier et al. (2015) interviewed a small number of fraud victims as well as professionals from different agencies dealing with fraud and found that victims saw the small amount asked for by the scammer as 'worth the risk' of winning the big prize. This is also present in some romance scams. Some romance scam victims view the experience as a near win, hoping that the next person will be a genuine love interest (Whitty, 2013). In addition, Fischer et al. (2013) found that victims often recall positive emotions and the size of the prize when talking about the experience, which suggests that positive emotions may detract from the assessment of risk when it comes to scams. This is consistent with Greenspan's (2009) model of gullible action, which suggests that decisions made in the presence of strong emotions are less likely to be rational and therefore, more likely to lead to gullible action.

Fischer, Jonas, Frey and Kastenmüller (2008) asked participants to make decisions on probability-based (risky) or fixed investment (definite) outcomes after asking them to read a passage about the investor facing a loss. The decisions presented to participants

to choose from were designed to concentrate on gains or losses. They found that participants in gains condition chose fixed outcomes and those in condition concentrating on losses chose probability-based outcomes. Participants were then told there was additional information available to them (short articles), some of which contradicted risky options and some, which contradicted definite outcomes, which they could use to make a final decision. Fischer et al. (2008) found that participants in gain condition chose more information that was consistent with their decisions, than inconsistent. They suggest that when people make decisions with losses instead of gains in mind they were less likely to exhibit confirmation bias (i.e. the tendency to interpret information as confirmation of their beliefs). Therefore, it seems that although some victims are aware there may be risks involved with certain offers, they purposely choose to concentrate on the positive rather than negative aspects. Scam victimisation in some instances might therefore be influenced by contributory emotional effects, such as excitement at a prospect of winning a prize (Lea et al., 2009).

Some scam victims may simply be attracted to scam offers. Research found that people who are not tempted by small amounts are also not tempted by larger amounts whereas repeat fraud victims are attracted to scam offers and more motivated to respond, despite otherwise making good decisions (Fischer et al., 2013; Lea et al., 2009).

2.5.5 Trust and gullibility

In their review of literature on trust, Rousseau, Sitkin, Burt and Camerer (1998) defined trust as "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" (p.395). They suggest that trust is a psychological condition that can cause or be the result of certain behaviour (e.g. cooperation) or a certain choice (e.g. taking a risk) and that without risk, trust would not be needed. Therefore, trust entails accepting the uncertainty when it comes to intentions and motives of others (Kramer, 1999). Nowhere is that more true than dealing with purchases on the Internet, where this uncertainty is multiplied. In order for a scam to be successful, the scammer or the scam offer must appear trustworthy. In their study, Grazioli and Jarvenpaa (2000) demonstrated how trust is enhanced on fraudulent websites, through specific manipulations, and how this impacts risk perceptions. Participants were asked to imagine a friend asked them for advice about a purchase and were then asked to review a website the friend wanted to purchase a laptop from. Half the participants were directed to a real website and half were directed

to a cloned website created for the purpose of the study, which contained manipulations to increase trust, such as third-party seal of approval, unlimited warranty, fake news clips praising the shop, customer testimonials etc. All of the manipulations were created to raise suspicion, such as the third-party seal of approval did not have the company registered on their website, customer reviews had discrepancies, links to the magazines quoted did not exist etc. Grazioli and Jarvenpaa found that only a very small number of participants rated the website as fraudulent, in fact the warranties given on the fake website were seen as more assuring than warranties on the legitimate site, as were the seals of approval, and this influenced the perceived risk. Similarly, Kim, Ferrin and Rao (2008) found that consumers' purchasing intentions are affected by trust. Third party seals (e.g. endorsements by other bodies), reputation, product information quality as well as privacy or security protection offered by the vendor, influence trust. They also found that with greater perceived risk, intention to purchase diminishes, however perceived benefit (e.g. a good deal) may increase the intention to purchase even when trust is low.

Langenderfer and Shimp (2001) argue that gullibility and a trusting nature distinguish scam victims from non-victims. Rather than examine a scam offer carefully, a victim may concentrate on how trustworthy the scammer appears to be. Greenspan (2009) suggests that gullibility involves trusting someone or something. It is more prevalent in children and those with cognitive impairment and learning difficulties, which is why the existing laws have special measures for protection of such populations. Gullibility may also be applied to fraud victimisation in certain contexts. For example, Greenspan (2009) argues that even smart people can sometimes engage in gullible action (i.e. acts that are against individual's best interests) due to certain situational, cognitive or personality factors, or the emotional state they are in (Figure 2.5).

Other research reports that fraud victims believe that the reason they were defrauded was down to them being too trusting or naive (Whitty & Buchanan, 2012b). This is consistent with Fischer et al. (2013). By using transcripts of interviews with victims of fraud, they text mined for words that reoccur frequently and found that participants often alluded to the trustworthiness of the scammer. Additionally, Fischer et al. (2013) conducted a large-scale survey, using self-constructed short scales to measure different psychological constructs, one of which included trust. They found that scam

compliance, measured by asking participants about previous fraud victimisation was associated with the trust in the scammer (also Workman, 2008).

The research by Evans and Revelle (2008) shows that trust may be influenced by personality traits as well as situational factors, such as reciprocity, which is a known scamming technique. It may also support Greenspan (2009) model of gullible action, which cites trusting nature as a possible personality trait that, in combination with other factors, could influence propensity to engage in a gullible act.

Is trust connected to gullibility? Rousseau et al. (1998) suggest that trust would not be needed if outcomes were certain; therefore, risk creates an opportunity for trust, and trust leads to risk taking. The connection between risk and trust occurs in reciprocal relationships, due to the uncertainty of the other's behaviour (i.e. if the other will act appropriately). Luhman (2000) suggests that trust is a component of cooperative relationships, and that without it, many daily activities would be severely limited. For example, trust is extended each time people shop online, as the goods paid for are not immediately collected. Instead, we take a risk and trust others to fulfil their obligation by sending the goods that were paid for. Although it is clear how scammers may exploit the extended trust in such situations, is trusting others an indication of gullibility? Rotter (1980) argues that trusting someone in the absence of warning signs is not the same as trusting someone in the presence of warning signs or evidence that the person is not trustworthy, and that only the latter is connected to gullibility.

This is supported by Markóczy (2003), who found that people high on trust differ in the amount of vigilance they exhibit and that vigilance makes a difference in how prudent one is likely to be in the situations when they have to predict other's behaviour. Markóczy (2003) used the electricity shortages in California to examine if higher trust would make participants better or worse at predicting others' behaviour. The capping of prices led to blackouts in certain parts of California during the excessive demand. Not in a position to increase the supply, the only way out of the blackouts was through appeal for voluntary reduction in electricity usage, causing a widespread social dilemma as people needed to sacrifice their usage for the greater good (i.e. so there would be no blackouts). Participants were given a statement measuring their beliefs of how their behaviour compares to others in regards to electricity usage. These were then compared with the participant's actual electricity usage and those of others. Accuracy of

expectations of others' behaviour was measured by how accurately participants predicted the cooperation of others to reduce their electricity usage.

As well as measuring trust, Markóczy (2003) gave participants a vigilance scale and found that people high on trust differ in the amount of vigilance they display. Those high on trust but low on vigilance were categorised as 'naive trusters' and those high on trust and vigilance were categorised as 'prudent trusters'. Prudent trusters (i.e. high in vigilance) were found to be better at correctly predicting others' behaviour.

2.5.6 Other individual differences implicated in fraud victimisation

Other individual differences connected to fraud vulnerability that have been considered in previous research include: greed, being fantasy prone or susceptible to flattery, having romantic beliefs, being easily intimidated and a tendency to act without deliberation (e.g. Buchanan & Whitty, 2013; Holtfreter et al., 2008; Langenderfer & Shimp, 2001; Whiteside & Lynam, 2001; Whitty, 2013).

2.5.7 Behaviours that enhance vulnerability to fraud

The research examined so far in this review suggests that there are certain behaviours that may enhance the risk of fraud victimisation. Titus, Heinzelmann and Boyle (1995) conducted a large-scale telephone survey, asking people about fraud victimisation and the specific details of frauds they had encountered.

The same data were used for a review on fraud victimisation by Titus and Gover (2001), who identified that joining online groups, entering contests and free prizes, making purchases on the internet or over the phone and even giving to charity as behaviours that increase the likelihood of fraud victimisation. Use of social media is a popular way of staying in touch with friends and sharing our experiences with others around the world. This means that personal data is available to wider audiences and this may increase the likelihood of being targeted by fraudulent offers (Parish et al., 2009). Another behaviour associated with vulnerability to phishing attacks is sharing and sending links via social media, as it is not always easy to discern what is a legitimate link and what may be a phishing attempt (Frauenstein & Flowerday, 2016).

2.5.8 Life circumstances and fraud vulnerability

Some research has also suggested that loneliness might also be a factor implicated in fraud victimisation. For example, Langenderfer and Shimp (2001) found that elderly

scam victims, although socially active, were more likely to live alone than non-victims (also Olivier et al., 2015). However, research by Buchanan and Whitty (2014) failed to find a relationship between loneliness and romance fraud victimisation.

Ageing has been associated in vulnerability to fraud. Langenderfer and Shimp (2001) suggest that reduced cognitive abilities are a part of an ageing process and due to this, elderly people are more prone to being defrauded. This is consistent with Smith (1999), who, in his review of fraud literature, suggested that dementia in elderly people leaves them open to being deceived and manipulated by scammers. He also found cases of financial fraud perpetrated against elderly people by those appointed as legal guardians or agents managing their financial affairs.

Some research has found that elderly people are more likely to be lonely or socially isolated, which enhances their vulnerability (Lea et al., 2009). Other authors have suggested otherwise; for example, James, Boyle and Bennett (2014) used data from a longitudinal study looking into conditions of ageing to examine correlates of susceptibility to scams. Participants were elderly adults without dementia. Susceptibility to scams was measured with questionnaire items relating to unsolicited phone calls by telemarketers as well as awareness that people over 65 tend to be targeted by scammers. Participants were also given tests to measure cognitive function, depression, health and financial literacy. They found that those most susceptible to scams were older participants, those with lower levels of cognitive function and lower levels of psychological well-being, as well as those with poorer health and financial literacy. These findings were irrespective of the educational and income levels of the participant. Regardless of their cognitive abilities, knowledge of financial concepts helped to prevent scam victimisation, as false information is rejected. James et al. (2014) also argued that the idea that vulnerability to scams in elderly people is down to them being socially isolated and physically frail is wrong, as these variables were not associated with susceptibility to scams in their study, and that active, healthy elderly people were equally susceptible.

Research also suggests that elderly people tend to be targeted by scammers more than other age groups (Harries, Davies, Gilhooly, Gilhooly & Cairns, 2013; Muscat, James & Graycar, 2002; Reisig & Holtfreter, 2013) and that this increases the likelihood of fraud victimisation. However, some research has produced different findings. Kerley

and Copes (2002) conducted phone interviews in which they asked participants about previous fraud victimisation and reporting behaviour. They found that elderly participants who are not property owners and lack financial stability were the least likely to be defrauded and suggested that this may make them less suitable targets for scammers. Titus et al. (1995) also found that elderly people are less likely to be defrauded and suggest that fraud victimisation cannot be predicted by demographics.

Certain life circumstances, such as a major medical treatment, marriage, birth or death in the family may also increase the likelihood of being targeted by scammers as this information is often kept by legitimate and illegitimate businesses to target consumers with specific offers (Titus et al., 1995; Titus and Gover, 2001). This may mean that younger populations may have reduced exposure to fraudulent offers, as they will have experienced fewer life events outlined above, across their lifespan.

Life events, such as bereavement, divorce or illness in the family may lead to extreme emotional vulnerability, which is then exploited by scammers. For example, Olivier et al. (2015) found that some victims engaged in scams because at the time, they were emotionally vulnerable or socially isolated. The communication allowed them to escape their grief, as regular contact with a sympathetic scammer was comforting. It also provided a meaningful activity. Titus and Gover (2001) argue that likelihood of engaging with fraud offers comes down to personality characteristics, demographics and life events.

2.6 Methodology in fraud research

Fraud victimisation has been researched extensively in recent times, allowing for better understanding of factors that influence vulnerability to fraud. However, measuring fraud compliance in a research setting is not easy without simulating fraudulent activities, which raises serious ethical considerations, but new approaches to investigating fraud are emerging as fraud continues to thrive. Table 2.4 outlines some of the key methodologies used by researchers examining fraud, which are then discussed below.

Table 2.4
Methodology in fraud research

Methodology	Research study
Interviews and focus groups with fraud victims and their friends and family	Button et al. (2009b), Button et al. (2013), Button et al. (2015), Cross (2013, 2015), Fischer et al. (2013), Olivier et al. (2015), Whitty and Buchanan (2012a), Whitty (2013)
Interviews with professionals and experts working with fraud victims	Button et al. (2012), Langenderfer & Shimp (2001), Olivier et al. (2015)
Phone or online surveys looking at fraud victimisation in general population	Buchanan and Whitty (2014), Holtfreter et al. (2008), Hutchings and Hayes (2008), Kerley and Copes (2002)
Interviews with representatives of private sector (e.g. banks) and public sector (e.g. Trading Standards)	Button et al. (2012)
Interviews and surveys with law enforcement bodies or professionals and analysis of existing crime surveys or longitudinal studies	Button et al. (2012), James et al. (2014), Muscat et al. (2000)
Examining postal and online scam content	Chang and Chong (2010), Lea et al. (2009), Nikiforova and Gregory (2013), Rege (2009), Whitty and Buchanan (2012a)
Using hypothetical scam situations	Modic and Lea (2012), Modic and Lea (2013)
Simulating a scam situation	Fischer et al. (2013), Jagatic et al. (2007), Lea et al. (2009), Scheibe et al., 2014, Workman (2008),
Existing personality measures used to compare to fraud victimisation or test fraud compliance	Buchanan and Whitty (2014), Modic and Lea (2012), Workman (2008)
Purpose built measures used to compare to fraud victimisation or test fraud compliance	Fischer et al. (2013), Modic and Lea (2013)

2.6.1 Interviews with victims of fraud and family members

Many studies have found interviews with victims of fraud to be an effective way of gathering data on processes that underline fraud victimisation (e.g. Button et al., 2013; Lea et al., 2009; Olivier et al., 2015; Whitty, 2013). Interviews access the rich details of individuals' experiences during and after fraud victimisation and the data can be used in variety of ways, either by generating themes and subthemes of the process or constructing typologies. Interview transcripts have also been used to data mine for the words related to fraud experience that occur most often through the interviews. For example, Fischer et al. (2013) used the interviews conducted by Lea et al., (2009) for data mining, to create psychologically meaningful categories or themes, running

through the interview transcripts. They found evidence of certain psychological processes recurring frequently through fraud literature; positive emotions and the size of the prize referring to superficial processing; trust cues and securing behavioural commitment. In depth interviews can, therefore, be a good way to gather information on psychological processes that underlie scam compliance, however, they can be time consuming to execute and transcribe.

2.6.2 Analysis of the scam content

Analysing scam content and communication has proven to be a good way of examining the latest techniques scammers employ when they contact the victim. Lea et al. (2009) were able to collect and analyse a large number of scam letters, such as scams purporting to be lotteries, prize draws, business opportunities, clairvoyants offering their services etc. They were able to identify specific psychological techniques scammers use in scam correspondence, such as urgency, social proof, authority, evoking visceral influence, soliciting small commitments from the victim to influence bigger commitments later on etc. Fischer et al. (2013) also examined a large corpus of scam communication including mailings, emails and website content and used text mining to categorise words recurring in scam correspondence. This enabled them to examine, which techniques appeared most frequently in scam correspondence. One important finding from their study was that these categories enabled them to see that although cues to scarcity and uniqueness are frequently used in scam correspondence, this was not picked up in the interview with fraud victims. Fischer et al. (2013) suggest that it could be that scammers use this technique even though it may not be effective, or victims may be influenced by them but may not be aware of that influence.
Text mining seems to be an effective way to process and categorise data collected by different methods, in order to explore shared commonalities.

Chang and Chong (2010) analysed the content of different fraudulent e-mails and found that these coercive techniques are also used in online communications. Whitty and Buchanan (2012a) studied internet posts on the romance fraud support site and were able to gain insight into how the scams work as victims posted details of the fraud online.

2.6.3 Hypothetical scam scenarios

Modic and Lea (2012, 2013) conducted research in which participants were given personality measures, after which they were asked to consider different text-based scenarios that could potentially be fraudulent situations. These included written descriptions of an online auction, a phishing bank email, a potential romance scam communication, a Nigerian or 419 scam, and a pyramid scheme. Participants were asked to decide how likely it was that each situation was a scam, how likely is it that people would respond favourably to it and if they had ever found themselves in such a situation, or responded to and lost money to such a situation. Although these studies are one of the first that specifically looked at scam compliance and personal characteristics, using hypothetical scam scenarios presents certain problems. In the first study, participants were asked to report if they have previously responded and lost money to the scenarios presented, measuring scam compliance over their lifetime, while personality characteristics were measured in the moment. The authors tried to control for this in their second study by asking participants to report if they had responded to and lost money to such a situation in the last three years but this still does not measure scam compliance in a given moment.

Additionally, the study reported that not many participants reported losing money to the specific situations mentioned, therefore compliance was measured by previous response or loss of funds to given scenarios. A possible problem with this may be that although responding to scam correspondence often leads to becoming a victim, this may not always be true for every scam situation in the Modic and Lea (2012, 2013) studies. Some scenarios were more obvious fraudulent situations, such as Nigerian scam or a pyramid scheme, while others were ordinary life situations that could be exploited by scammers. For example, responding to someone regarding a classified advert or an online auction may not be the same as responding to an unsolicited Nigerian scam offering rewards for help with transferring funds or to a letter stating a lottery win. The events used may not therefore, have equal prevalence in society. Some fraudulent situations closely mimic real-life situations, such as offering items to buy in online auctions, therefore the only way one may realise it is a scam is after some correspondence with the scammer. Therefore, in some situations, responding to a real-life situation, which could also be fraudulent, may not necessarily lead to greater scam compliance. Another possible problem with this methodology is that people may not

always know if the real-life situation they responded to was indeed, fraudulent or not, unless they lose funds.

Asking participants to report how they would behave in a potential scam situation may not be an accurate way of predicting what people would actually do when they find themselves in a fraudulent situation, especially as some scams are increasingly sophisticated. Although using scam scenarios may not be the ideal way to capture scam compliance, these studies were one of the first to try to experimentally explore individual differences implicated in compliance with fraudulent offers.

2.6.4 Simulating scam situations

Several researchers have attempted to simulate a real-life scam situation in order to examine how people behave when they encounter scam communications (Fischer et al., 2013; Jagatic et al., 2007; Lea et al., 2009; Scheibe et al., 2014). What people think they would do in a certain situation and what they actually do in such a situation is often incongruent, therefore simulating scam situations may be a good way of capturing people's behaviour in real scam situations.

Lea et al. (2009) sent unsuspecting participants scam type offers in two separate studies. In one, participants received a letter with a simulated prize draw and a questionnaire asking about their reaction to it and in the other, participants were sent the same type of scam simulation but the questionnaire was not immediately apparent. Only if the participants were sufficiently interested to read about the scam offer, would they find the questionnaire asking for their reactions. Lea et al. (2009) suggest that the first study was able to capture cold responses or what people are likely to do and the second study was able to capture hot responses or how people felt whilst they evaluated the offer. The scam content was manipulated to look official or not, the prize was manipulated to be large or moderate, and some included visceral triggers whilst others did not.
They found that when reflecting on the scam communication (cold response), people reported being influenced by the size of the prize but this was not evident in the second study measuring hot responses, where significant effects were down to content cues, such as visceral triggers and official status. These studies indicate that people may think they know what would influence them in a certain situation; however, the psychological techniques used by scammers may be more subliminal.

Jagatic et al. (2007) also simulated a phishing attack, coming from a friend and coming from a stranger, and found that that phishing emails were more successful when coming from a friend. But additional data came from a blog they created for participants after debriefing, so that they could discuss the study. The blog posts showed that several participants expressed anger and called the experiment fraudulent and unethical, illustrating that many participants felt their privacy had been violated. This demonstrates that fraudulent attacks, even when no funds are lost, have an impact on victims. Although the blog comments were plentiful, no participants who left comments admitted they have been phished, despite 77 out of 96 participants falling for the phishing attack coming from a friend. Jagatic et al. (2007) argues that this denial illustrates that people often do not want to admit their own vulnerability. Many participants also did not understand that publically posted personal information is easily accessible to fraudsters who may use it to influence scam compliance.
These findings highlight the fact that much can be gained from simulating fraud situations in order to examine how people behave when they are presented with real life situation, rather than with a hypothetical one. However, there are ethical implications in conducting studies where participants are scammed as Jagatic et al. (2007) study shows.

Scheibe et al. (2014) aimed to conduct a study that would mimic a real telemarketing scam but which would take ethical implications into consideration. Some of the unsuspecting participants were called and warned about a certain scam only, while others were warned about different scams. Weeks later, the same participants, as well as others that were not forewarned about the scam, were called by a telemarketer offering to sell an information package, which would allow participants to apply for a governmental stimulus grant. Since collecting the payment on the spot would have been unethical, an agreement to receive a package and pay a fee was taken as a compliance with the scam instead. However, this means that the number of participants that would have honoured the agreement by sending the payment remains unknown. Although the study found that forewarning about scams may be effective fraud prevention, difficulty in knowing how many participants would have agreed to pay the fee on the spot (i.e. comply with the scam) means that the generalisability of the results is limited. For example, positive emotions associated with the attractive offer (i.e. hot response) may wane by the time participants receive the information package with an invoice, making the offer less attractive. Therefore, conducting ethical experiments, which mimic real life scam situations is extremely difficult.

2.6.5 Self-constructed and personality measures in fraud research

The research reviewed in this chapter suggests that personal characteristics may play a part in individual vulnerability to fraud. Therefore, further research in this area is needed in order to improve advice given to victims of fraud in order to prevent repeat victimisation. This would also benefit those that have not been defrauded as yet, to understand their vulnerabilities. It is evident from existing literature and crime data, that fraudsters are becoming more sophisticated in their approaches and using psychological techniques in order to enhance compliance, often specifically targeting desired victims.

Research by Modic and Lea (2012, 2013) explored personality characteristics with regards to scam compliance. They gave participants numerous psychometric measures in order to assess what personality traits may influence scam compliance. In their first study this included a measure of self-control, the Big-5 personality measure and a measure of impulsivity and in their second study, the newly developed Susceptibility to Persuasion scale, which consisted of four subscales; authority, social influence, consistency and self-control. Participants also received descriptions of real life scenarios that could end in fraud victimisation and were asked if they had responded and lost money to each scenario given to them to evaluate. Due to a lack of participants that lost money to hypothetical scenarios, scam compliance was measured by whether participants responded to fraudulent scenarios in the past. The studies found several predictors of scam compliance, including extraversion, premeditation and agreeableness (Modic and Lea, 2012), and in the subsequent study; lack of self-control, authority, social influence and need for consistency (Modic and Lea, 2013). Modic and Anderson (2014a) further developed their Susceptibility to Persuasion scale, by using items from existing measures, containing 10 subscales; premeditation, consistency, sensation seeking, self-control, social influence, similarity, risk preferences, attitudes towards advertising, need for cognition and uniqueness. The scale has not been experimentally tested in real contexts.

One of the studies conducted by Lea et al. (2009), used self-constructed short scales to measure different psychological constructs. Participants were asked about previous fraud victimisation and feelings about receiving scam offers in the past, if no victimisation occurred. Analysing the data from this study, Fischer et al. (2013) found several psychological constructs, such as high motivation, positive emotions, trust, susceptibility to persuasion, susceptibility to social influence, scarcity, confidence in

knowledge etc. Fischer et al. (2013) also found that scam compliance, measured by asking participants about previous fraud victimisation, was associated with high motivation (e.g. size of the scam offer), positive emotions, trust in the scammer and susceptibility to persuasion. While it is encouraging to see the use of self-constructed items created specifically to address scams, previous fraud victimisation is not an ideal measure of general scam compliance. Although repeat victimisation is common in some fraud victims, there are many victims of fraud that become more aware of fraudulent practices following fraud victimisation. Therefore, a measure of scam compliance, such as a simulated scam situation, in conjunction with individual characteristics measures, such as those used by Modic and Lea (2012, 2013) would be beneficial.

2.7 Summary

The wealth of research discussed in this chapter has shown that scammers are getting increasingly sophisticated in orchestrating scams that exploit human attributes, behaviours and circumstances. As fraud perpetrated online, over the phone and via postal means, becomes increasingly difficult to investigate and solve due to the cross-border element, the number of victims is likely to soar, causing great distress to victims and their families. Therefore, it is paramount that fraud prevention focuses on the right messages and targets the right audience. Although many people are aware of dangers of fraud, not many people are aware of the underlying factors that govern scam compliance, some of which are evoked by sophisticated scamming techniques, or in what way their individual attributes make them more likely to respond or comply with fraudulent offers. Several different forms of scam influence as well as individual attributes, circumstances and behaviours that seem to influence or moderate scam compliance have been identified in this chapter and are summarised in Table 2.5. In addition, several theoretical models and theories have been proposed in order to explain how these different vulnerability factors, when combined, influence scam compliance, indicating that individual attributes may be facilitating or moderating vulnerability to fraudulent offers (Greenspan, 2008; Langenderfer & Shimp, 2001; Parish et al., 2009). However, despite this, there are, at present, no widely used measures that measure individual attributes associated with susceptibility to fraud. The present thesis aims to

develop and test a psychometric measure, which might pinpoint areas of individual's vulnerability to fraud.

Table 2.5.
Scam techniques, individual differences, behaviours and circumstances implicated in vulnerability to fraudulent attacks

Scam techniques	**Individual differences**	**Behaviours**	**Circumstances**
Visceral influence	Self-control	Use of social media	Living alone
Liking and similarity	Impulsivity and Premeditation	Online or phone purchases	Ageing
Evoking social norms	Background and scam knowledge	Entering contest and free prizes	Bereavement or divorce
Authority	Information processing	Giving to charity	Marriage, birth or death
Scarcity and urgency	Assessing risks		Major medical treatment or illness
Social proof and social influence	Sensation seeking		
Commitment and consistency	Trust and gullibility		
Dishonesty and distraction principles			

In addition, much of fraud prevention and the Internet security advice are disregarded, whether because people are used to such advice and are no longer paying attention to it or due to the fact they find it does not apply to them. For example, Fischer et al. (2013) found that while some scam techniques work for some people, they do not work for others, therefore it is reasonable to assume that people discard certain advice because they may feel that it does not apply to them. Egelman and Peer (2015) found individual differences to be connected to privacy attitudes, and suggested that security warnings may be more effective if they considered user's individual traits and were framed in a way that works for a given user. Therefore, fraud prevention may be improved by identifying individual attributes implicated in vulnerability to fraud and making fraud advice more personal and possibly more interesting. However, this is currently missing. One reason for this gap might be down to difficulty in studying scams. While interviews with fraud victims are a good way of identifying possible attributes that made them more likely to comply with the scam, developing and testing a measure

which would identify these attributes is challenging. As previous studies have found (Jagatic, et al., 2007; Modic & Lea, 2013; Scheibe et al., 2014), measuring scam compliance is difficult without employing unethical practices (e.g. deception and persuasion), such as those used by scammers. As Jagatic et al. (2007) have found, this has a potential to cause distress to participants, especially if participants were selected without asking for consent. Therefore, frequently, different scam simulations have been used, however, this may mean that the results may not represent what people would do in a real-life scam situation. The present thesis aims to address some of the limitations affecting the measurement of scam compliance.

2.8 Thesis aims

The aim of this thesis was to examine individual differences that might predict susceptibility to fraud, and in doing so whether an individual difference approach is suitable to the study of fraud victimisation. In order to do that, the present thesis draws from a wide range of fraud research, as well as relevant theories and theoretical models and builds on research looking into individual attributes as predictors of scam compliance (Modic & Lea, 2012, 2013). The general aim of this programme of research may be broken down into 3 related primary aims:

- To identify factors and personal attributes which contribute to making judgment errors in scam situations by conducting interviews with victims and near victims of fraud (Study1, Chapter 3).
- To construct and develop a psychometric questionnaire designed to indicate an area of individual susceptibility to fraudulent offers (Study 2, Chapter 4).
- To test the utility of the newly developed measure of fraud on a proxy scam situation (Study 3, Chapter 5).

The measurement and evaluation of the factors underlying compliance with fraudulent offers are important for a number of reasons. The measure can be a practical way of engaging victims and potential victims of fraud to take an active role in fraud prevention by understanding their own vulnerability when it comes to fraudulent offers. It may offer a way of indicating individual strengths and weaknesses, allowing for more tailor-made advice that could be combined with awareness of scamming techniques that

exploit certain individual attributes. This would allow for incorporation of external as well as internal factors that contribute to scam compliance and offer a better protection than general scam prevention advice. Finally, fraud prevention practitioners could use the measure as an instrument for evaluating the vulnerability of the victim when fraud is reported, in order to determine what course of action may be most suitable.

Chapter 3

The voices of scam victims: A psychological model of the experience of fraud

3.1 Introduction

This chapter explores the psychological precursors and personal consequences of fraud through interviews with victims of fraud. Exposure to fraudulent schemes, cons or scams has become a widespread experience for individuals within modern society. Whilst many forms of scams are known to predate widespread use of the Internet (Glickman, 2005; Zuckoff, 2005), the ease and anonymity of online communication has undoubtedly increased the range of fraudulent offers, increasing the volume of people who are potentially exposed (Smith, 2010). In addition, well-known scams, (e.g. Nigerian scams) may now be used by scammers to identify and target the most vulnerable individuals (Herley, 2012). The Internet not only affords fraudsters greater anonymity but also distances the perpetrator from the victim, resulting in reduced empathy for the victim. As a result, fraud is thriving. The UK Annual Fraud Indicator estimates a total annual loss to the economy due to fraud of around £190 billion, with individual losses of around £6.8 billion (Button et al., 2017). In addition, the number of fraud offences recorded in England and Wales by the National Fraud Intelligence Bureau in 2016, rose to 641,535; largely driven by online banking and non-investment fraud (Office for National Statistics, 2017). Given that cost estimates are based only on certain categories of fraud and that many instances of fraud are often not reported by victims, it is likely the true personal losses arising from individual fraud will be higher.

3.1.1 Factors that contribute to fraud victimisation

The risk of being targeted by fraudsters has been shown to vary across different life circumstances. For example, entering prize draws, reaching retirement age, moving home, making big purchases, buying insurance, medical treatment, marriage, and the occurrence of births or deaths in the family have all been shown to increase risk (Titus et al, 1995; Titus & Gover, 2001). The personal vulnerability created by such events is attractive to scammers who may actively search for people in these categories.

Several psychological traits have also been identified which may directly lessen protection from a fraud once presented, or indirectly through their influence on life events (Parrish et al., 2009). People who are susceptible to flattery, easily intimidated, who possess risk-taking tendencies or exhibit less self-control have been found more prone to being defrauded (Holtfreter et al., 2008; Schreck, 1999). Langenderfer and Shimp (2001) have similarly identified lack of self-control as a factor in vulnerability to

scams but suggest that scepticism and greater knowledge about scams may moderate vulnerability. A disinterest in current affairs and carelessness of information processing also seem to offer advantages to scammers since individuals are less likely to learn from news about current fraud practices (Titus et al., 1995).

A number of dispositional differences between victims and non-victims have also been identified, including positive emotional reactions to high-value incentives, a reliance on signs of authority and self-confidence (Fischer et al., 2013; Langenderfer & Shimp, 2001; Lea et al., 2009). Previous scam victims have also been shown to exhibit greater susceptibility to social influence and a greater need for consistency with their own preferences in order to commit to an offer. Reduced premeditation, or a lack of deliberation when making decisions, was also found to be highly predictive of scam compliance (Modic & Lea, 2012, 2013). As fraud is increasingly prevalent and difficult to investigate and prosecute, as well as having a financial and psychological impact on victims (Button et al., 2010, 2012, 2014; Cross et al., 2014; Whitty & Buchanan, 2012b; Whitty & Buchanan, 2016), taking an individual approach to understanding processes that govern compliance with fraudulent offers could assist future fraud prevention and educational measures and potentially reduce the number of victims.

3.1.2 Research aims and rationale

The present study explores the interplay of factors in scam events using a narrative approach, with the events reconstructed from the victim's perspective.
The main aims of this study are:

- To ascertain what processes underlie scam compliance and identify factors (if any) that facilitate or moderate fraud vulnerability
- To organise the newly gathered data into themes and subthemes associated with vulnerability to fraudulent offers
- To use the themes and subthemes as a guide to help inform questionnaire development in the subsequent study

Interviews enable exploration of complex issues that are difficult to capture through quantitative means (Burman, 1994). As such, interviews have been proven to be an effective way of gathering data on processes that underlie fraud victimisation (Button et al., 2013; Cross, 2013, 2015; Fischer et al., 2013; Lea et al., 2009; Olivier et al., 2015;

Whitty, 2013; Whitty & Buchanan, 2012a). Interview transcripts have been used in a variety of ways: as a way of generating themes and subthemes to identify the key elements needed to explain the research phenomena, to construct typologies or to mine for recurrence of certain words (Cross, 2015; Fischer et al., 2013; Whitty, 2013). As such, they were deemed as the most appropriate method for exploring intricacies of the scam process and the eventual reasons for compliance.

3.2 Methods

Scam narratives were gathered through twelve semi-structured interviews designed to cover specific themes, however, natural story telling was encouraged. Narratives incorporate the facts and the individual's making sense of them as they unfold, preserving the interrelations between different facets of one's life and the scam that lead to certain outcomes. Furthermore, alongside the recollections of past events, narratives present psychological scenarios relative to different moments in the scam process, crucially including the fantasies and future-oriented reasoning that the fraudulent offer might have elicited (Bruner, 2003). Whilst no claims are made about the factual truth of each and every detail recollected by the interviewees, experiences are uniquely positioned to offer pictures of how the scam had presented itself, had been lived through and was evaluated afterwards.

3.2.1 Participants

A total of 12 participants, 7 men and 5 women were interviewed. All interviewees were volunteers who were recruited by advertising the study through various social media sites, online fraud information and support sites, and direct email to students and employees within the University of Portsmouth. No participants were approached directly.

All participants had been victims of at least one scam. One victim had been able to recognise the fraud before losing funds. The extent of the financial loss and scam delivery method varied (i.e. online, phone, face-to-face). Details are presented in Table 3.1.

Table 3.1
Participant, scam and reporting path information

Participant†	Age	Occupation	Scam type	Amount lost / recouped	Reporting path
Chloe	26	Admin	Purchased tickets from a fraudulent website	Lost: £190 Recouped: £0	Bank
Bill	35	Design	Defrauded in the street by a scammer who asked to change money	Lost: £20 Recouped: £0	Not reported
Kate	46	IT consultant	Invested in a pyramid scheme through a friend	Lost: £500 Recouped: £0	Not reported
Robin	50	IT consultant	Invested in a pyramid scheme through a friend with Kate	Lost: £500 Recouped: £0	Not reported
Peter	52	Out of work due to disability	Approached by a scammer pretending to be a mechanic offering to fix his car	Lost: £60 Recouped: £0	Not reported
Rob	57	Software engineer	Bought a heavy goods vehicle training from a fraudulent company	Lost: £1200 Recouped: £0	Police, AF, TS, Civil court, PHSO
Greg	27	Researcher	Realised it was a scam when booking a travel tour abroad	Lost: £0 Recouped: £0	Not reported
Jane	41	Book editor	Paid for a passport and driving license on a fraudulent website	Lost: £90 Recouped: £0	Not reported
Henry	64	Artist	Invested in shares of a fraudulent company after being contacted by telephone	Lost: £25,000 Recouped: £0	Police, FCA, solicitor
Nina	44	Accounts	Bought items from a fraudulent website and received only part of the order	Lost: £200 Recouped: £75	PayPal and Mastercard
Fred	26	Construction	Bought a camper van on eBay and paid through the fake PayPal invoice asking for a bank transfer	Lost: £3500 Recouped: £0	Bank, eBay, PayPal, AF
Sam	34	Sales	Bought a job training pack after being promised a job if she completed the training	Lost: £20 Recouped: £0	AF, Bank

Notes.
AF – Action Fraud
FCA – Financial Conduct Authority
TS – Trading Standards
PHSO – Parliamentary and Health Service Ombudsman
† Participant names have been altered to protect anonymity

3.2.1.1 Exclusion criteria

Participants under 18 years of age or those with mental impairment or mental illness were excluded due to their vulnerability, as outlined by British Psychological Society (BPS) code of ethics. Those over 65 years of age were also excluded based on previous research findings. Research suggests that those over the age of 60 are more likely to suffer diminishing cognitive functions that can be part of an ageing process (Callahan, Unverzagt, Hui, Perkins & Hendrie, 2002; Griffiths & Harmon, 2011; Langenderfer & Shimp, 2001; Zamarian, Sinz, Bonatti, Gamboz, & Delazer, 2008). Elderly people may also be more vulnerable due to other factors related to old age, such as loneliness and loss of independence (Martin, 2009), therefore they may not represent general population.

Victims of romantic scams were also excluded from the study, as romance scams have been extensively studied (Buchanan & Whitty, 2014; Whitty & Buchanan, 2012a, 2012b; Whitty, 2013; Whitty & Buchanan, 2016). They also differ from other scams in that they rely on the lengthy communication with the victim, which is akin to grooming (Whitty 2013). In addition, romance scams have been found to cause victims great distress so any recollection of events for research purposes, unless necessary, might have caused further distress.

3.2.2 Interviews

The study's aim was to explore personal, social and situational factors related to the scam event as they were seen by the interviewees. Due to the personal and potentially sensitive nature of the interviews, participants were given the option to be interviewed face-to-face or by telephone according to which they felt more comfortable with (Legard, Keegan & Ward, 2003). In some cases, face-to-face interview was not possible due to distance. As a result, 7 face-to-face and 5 phone interviews were conducted. The quality of the phone interviews was good, however, two interviews had few short inaudible periods. The interviews were designed to cover all stages of the scam process; beginning with the circumstances the victims found themselves in at the time. The natural flow of the story-telling was encouraged by asking participants to describe the experience from beginning to end and prompts were used to encourage and support participants to expand on their answers only where needed. Participants were also asked to reflect on their feelings during the experience, what they think made them vulnerable and what they think might have helped them to avoid such a situation in the

future. Finally, participants were asked about what they did upon discovering the fraud and about the emotional impact of the events. The main themes covered in the semi-structured interviews are shown in Table 3.2

Table 3.2
Interview schedule for Study 1

Type	Questions
Warm up	• Can you tell me something about yourself and your everyday life in general? • What kind of things do you enjoy doing in your spare time?
Main question	• Please can you tell me about what happened in the scam in as much detail as possible, starting with what was going on in your life at the time?
Questions to cover the themes	• What form did the communication take? (verbal/written?)
Communication	• What were your thoughts about the information you were given at the time? • How long did it go on for?
Scammer	• Please tell me as much as you can remember about the scammer? • What were your thoughts about the person you were dealing with? • How was it when you had contacts with them? • What was the tone of the exchange with them? • How did the relationship develop? • How did you feel about the relationship with them?
Processes	• Can you remember your feelings, emotions, gut feelings at the time? • What do you think led you to trust the situation/scammer?
Reflections	• Looking back at the events, what might have helped you to avoid it? • How did people close to you react when (if you did) you told them what had happened? If not, what are the reasons you didn't tell anyone? • Do you feel changed by the experience? In what way? (feelings, thoughts, attitudes) • Have you changed your behaviour in any way after this episode? How? • How do you feel now about speaking about your experience to others?
Ending questions	• Is there anything else you would like to tell me about your experience? • Are there any questions you feel are important to ask that I have not covered? • Did you experience any negative thoughts or feelings during the interview? Please tell me about it? What could I do different to minimise that in the future? • Do you still have the correspondence? May I have a look at that?

3.2.3 Data treatment and analysis

All interviews were audio recorded and transcribed verbatim without the use of software, retaining conversational features such as repetitions, hesitations, pauses and laughter. Any information that could potentially reveal the participant's identity was

changed or omitted (King & Horrocks, 2010; Kvale & Brinkmann, 2009). As a first step into the analysis, each interview was summarised to provide a synopsis and rendition of the key points covered. Despite differences in the range of frauds the interviewees had been victims of, from brief, single contact frauds causing the loss of limited sums of money to prolonged communication exchanges between the victim and perpetrator involving much higher financial loss, three stages to each scam process could be consistently identified for all, which included: 1) the precursors of the scam, 2) the committing to the scam and 3) the aftermath. Thematic analysis was then applied to the narrative segments relative to each stage (Braun & Clarke, 2006), in order to identify the main elements for each chronological stage of the scam, preserving their connection with the whole experience, in order to unearth what individual attributes contribute to fraud vulnerability. The quotes presented in this chapter were treated by removing word repetitions and speech overlap.

3.2.3.1 Coding

The first phase was familiarisation, which entailed reading and re-reading the interview transcripts. Units of meaning (excerpts that could be assigned a single code) were then identified and assigned preliminary codes. These were adjusted as the analysis proceeded; a first level of emerging themes and subthemes; that would grasp the essence of clusters of codes, were then formulated. An example of the coding process is outlined in Table 3.3.

Table 3.3
Examples of coding

Unit of meaning	**Preliminary codes**	**Emerging themes and subthemes**	**Final theme or subtheme**
I received the confirmation email, which looked to me very, kind of, official.	official legitimacy	Trusting legitimate looking material	Credibility and legitimacy
I feel like I was, in a way, stupid and I feel like I failed. I have failed.	feeling foolish failure	Erosion of self esteem	Psychological consequences
Most people that stop me, stop me to try and talk to me or I can detect any kind of request for anything uhm, are greeted by considerably less open and generous and understanding person than back then.	loss of trust, loss of empathy, consequence of fraud	Consequences of fraud Loss of trust in society	Loss of trust

A further examination of the interview transcripts was conducted in order to see

whether the themes were the best fit for the data, and if they represented, to a satisfactory level, the different trajectories narrated by the participants. The themes and subthemes were finalised in this stage.

3.3 Results

The primary themes and subthemes identified for each stage of the scam process are shown in Table 3.4 and presented in detail in the text below, illustrated with fragments from the participants' narratives.

Table 3.4
Stages, themes and subthemes of the fraud process

Stage	Primary Theme	Subthemes	Description
Precursors	Time constraints	Urgency Lack of time to consider information	Lack of time to consider the information needed and a preference to make a quick decision
	Dissatisfaction with one's present circumstances		Personal circumstances that make a scam offer appear more attractive (e.g. lack of funds)
	Social Influence		Opinions or backing of other people that has a bearing on the decision making
Commitment	Factors pertaining to the perpetrator	Credibility and legitimacy Similarity, familiarity and likeability Limited availability Urgency	Manipulations used by scammers in order to elicit compliance, such as appearing likeable and trustworthy, producing legitimate looking communications and limiting the time the offer is valid for
	Factors pertaining to the victim	Lack of scrutiny of available information Excitement Social norms	Factors influencing compliance, such as emotional reactions elicited by a scam offer, insufficient information processing and compliance due to social norms.

Stage	Primary Theme	Subthemes	Description
Aftermath	Psychological and financial consequences		Financial hardship and emotional distress experienced by victims
	Avoidance strategies		Behavioural changes implemented in order to avoid future victimisation
	Resolution and justice	Dealing with authorities Need for resolution	Difficulties and lack of attention experienced by fraud victims when fraud is reported to the authorities and a need for closure after fraud victimisation
	Loss of trust		Loss of trust in the authorities and the society as a whole

3.3.1 Precursors

This section presents the different sets of situational or personal circumstances that participants reported as driving their engagement with the fraudulent offer in the first place.

3.3.1.1 Time restraints and urgency

Time restraints refer to urgently needing to resolve a situation, purchase a product or a service. It also refers to the lack of time needed to carefully consider the information, which is not imposed by the scammer but rather by personal circumstances. Time restraints can lead to fraud victimisation even when people are usually cautious. Jane was in a rush to renew her passport and driving licence, and did not consider in detail all of the information on the website through which she paid for a service that should have been free of charge.

> Jane: "Uhm, in a kind of snatched 15 minutes I thought; right, I'm just gonna go online and I'm gonna sort it out before I pick up the kids from school. Uhm, so it was classic case of being in a hurry, and I uhm, clicked renew driving licence, uhm, online and I was, as many other people have been, directed to a false site. I read through it and thought; that's funny, I can't imagine why you have to pay to renew your driving licence, maybe that's changed, it's been such a long time since I had a driving licence uhm, so merrily clicked through uhm, and thought right, great, that's that ticked off my list." (P1, lines 28-35)

Jane's reconstruction portrays the conditions under which her purchase occurred, a common scene in the busy life of a parent who, using a limited time window to carry out a task that needed to be completed, follows the first link coming up on internet without checking its validity, despite being surprised by some elements of the procedure.

Situations of urgency can present in face-to-face scams as well. On returning to his car after shopping in a supermarket, Peter was met by a man who told him that his car engine was faulty as it had smoke coming out of it. As Peter has a physical disability, which means that he has difficulty standing for long periods of time, he accepted the man's offer to fix the car for a fee, only to find out later from a local newspaper, that this had been a scam. He explains his decision as follows:

> Peter: "Something at the back of my mind said; you are a member of a breakdown service, call them. But it was that time issue, you know. I would have to wait for them to arrive would have to wait for them to fix it, if they could fix it. Uhm, and that would mean waiting around. Uhm, I just wanted to get home." (P3, lines 130-133)

Similar to Jane's position before, Peter weighs time against the possibility of saving money, the desire to solve the situation rapidly stopping him from considering the possibility of the situation being inauthentic.

3.3.1.2 Dissatisfaction with one's present circumstances

A different type of precursor has to do with challenging life circumstances. The need or desire to improve the current situation often makes fraudulent offers look more attractive, so they may be grasped without too much reflection.

Desperate to find another job, Sam purchased a training pack online, under the promise that she would be offered a job if she completed the training. The training pack never arrived and Sam later discovered on the Internet that the company was fraudulent.

> Sam: "You see, unfortunately, the way I was feeling on Monday, had I seen it I probably would have still gone ahead with it coz sometimes you're feeling desperate, […] d'you understand what I mean? You don't feel, you don't think to think so clearly, your emotions running." (P5, lines 205-208)

Sam describes her state of mind as refusing to apply rational judgment even if she had

seen the information beforehand, hoping that the job might be genuine, as she was eager to change her circumstances.

Henry, a self-employed artist, invested a large amount buying shares in a bogus company, for similar reasons to Sam. Starting with five thousand pounds, after frequent conversations with the scammer, Henry was encouraged to take a loan for a further twenty thousand pounds. His circumstances at that particular time in his life, he says, made the scam look extremely appealing to him.

> Henry: "Uhm, my situation really is that it is pretty hand to mouth, uhm, you know, it's a precarious business being a self-employed artist as you might imagine, and I had brought up my family just about, from proceeds of my endeavours. And I got to this point in my life where I was living separately from my family, uhm. I was living alone, uhm, and work wasn't as forthcoming as it had been and there was an opportunity to make some money, is what it amounted to. [...] I was also going through some very difficult times with my wife, uhm, there was that dimension to it as well. Yeah, it's hard to fully articulate but I think it's possible that when you're stressed about one situation, your natural guards maybe not be in the position they would've been otherwise. And so you kind of embark on a route that leads you down a more troubled path than you might've taken had your err, instincts been at a finer tuned level." (P8, lines 385-391 and P11, lines 513-521)

Henry's reconstruction of what led him to embark on the scam, and persist in it, presents a more complicated picture; it did not only imply solving immediate financial issues but also alleviating the psychological hardship of prolonged financial uncertainties and relationship troubles. As he explains, he feels that stress and loneliness may have dulled his judgment, lowering the threshold at which his "natural guard" would be triggered.

3.3.1.3 Social influence

Life dissatisfaction may sharply increase vulnerability to fraud but this is by no means a necessary or sufficient condition for becoming a victim. Knowing that an opportunity has backing from other people, especially those from the same social circle, can be enough to raise interest and make someone commit to a fraudulent offer. Introduced to a pyramid scheme by close friends, Robin describes his reasoning when he decided to proceed despite his initial doubts.

> Interviewer: "So why would you say you went along with it? What would be the reason?"
>
> Robin: "To an extent it may have been [...] I don't know if some of it was peer pressure, and I

> don't mean that Mark was, that he and his partner were particularly pressuring us, it just, you know the peer pressure to fit in, to be part of the group, uhm, partly peer pressure, partly uhm, you know, it could work. It's only five hundred quid to find out if it works and if it works, you get seven and a half grand. [...] But yeah, I think it was probably peer pressure and conforming and little bit of greed. Thinking, you know, we may get something for nothing and then realising that, uhm, it's not for nothing." (P6, lines 286-303)

In societies permeated by individualistic values, it is easy to underestimate the extent to which social conformity, i.e. following the lead of others, plays a role in individual choices. Robin was introduced to a seemingly high-profit scheme by his close friends (who lost money just as he did). Despite his friends not being particularly insistent, he recalls a desire to "fit in", to act in accordance with his social circle.

Interestingly, Robin also described that being scammed with his friends meant he did not feel as humiliated about being scammed, as it was an experience shared with his peer group.

> Robin: "If you make the same mistake with somebody that you trust or somebody that you respect or somebody that you like uhm, you probably don't feel as humiliated, you don't feel as gullible." (P4, lines 151-153)

3.3.2 Commitment

Once initially attracted, staying engaged with a scam and eventual compliance to the point of financial loss relies on a varied set of factors; some of which pertain to the perpetrator and some to the victim. In this section, the different components that may influence scam engagement after the initial interest are explained.

3.3.2.1 Factors pertaining to the perpetrator

Scammers employ different techniques to entice their victims, some oriented to avoid generating suspicions, and others to enhance the desirability of their offer. Three strategies identified in participants' narratives that are used by scammers are considered below.

3.3.2.1.1 Credibility and legitimacy

The success of the scam relies on appearing trustworthy and legitimate as a means of avoiding suspicion. For example, scammers imitate genuine companies in their outlook,

whether face-to-face or online, create material that looks professional or adopt a respectable personal style. Online, this may include professional looking websites with credible content; face-to-face, scammers may appear immaculately presented, likeable and friendly, and generate positive first impressions.

The following illustrates how carefully credibility can be constructed. Rob needed a driving licence for a heavy goods vehicle (HGV) he had bought. The licence involves a training package, including lessons with an instructor that can be purchased online. Prior to paying by bank transfer, Rob checked the company he was dealing with on the UK Government's Companies House website. The company was registered and nothing stood out, but Rob found out later that the company was fraudulent.

> Rob: "Generally the companies are registered with Companies House, real companies, real people uhm, the directory pointing to the real director's address. But this company uhm, the company's registered address was a mailbox in Reading where they never had any contact. The only director that this company had is a completely fictitious person. The website registration was done through somebody that doesn't exist, uhm, and so their trading address was a firm of managed offices, uhm, where they never actually set foot in [...] and I was quite amazed that people could create a limited company, with completely fake addresses." (P2, lines 65-74)

Rob's account illustrates the ways scammers enhance the credibility of their offer by creating false information through trustworthy sources. Even a conscientious customer could be reassured, only to discover when things go wrong that such information might be fabricated and that even official websites are not exempt. Besides creating a legitimate commercial identity, the bogus company had also equipped itself with latest technology, projecting a picture of commercial success:

> Rob: "I noticed that he knew who I was right away. You'd call 0870 and he picks up the phone and says; hello Rob. My first impression on that was; ooh, these people have got customer management software, they've got phones connected to computers so when somebody calls straight away you've got customer details. I was quite impressed by that." (P8, lines 352-356)

A credible presentation, such as a good website with convincing logos, is a condition for engagement, as anything looking less than professional may raise suspicion. The example above, and a similar scam reported by another participant in which a foreign

company held a UK-based URL, show that scams can be extremely sophisticated in appearance. As the victims reported, only when typing 'fraud' or 'scam' in association with the company name or goods being sold, did bad reports appear on the Internet search engines. Moreover, this can be offset by online customer review sites carrying fake reviews of such companies in order to make the services they offer seem attractive.

Credibility as a pre-condition to scam success is influential in face-to-face situations as well, as the example below illustrates. On vacation in Brazil, Greg and a friend were trying to organise a tour of the Amazon, which proved difficult. Eventually, as Greg explains, they were persuaded by someone's credible demeanour.

> Greg: "The first impressions were that he was really nice, he was in a suit, he was well presented, he spoke good English. You imagine that you've got this nice, ehm, streets where they all sell Amazon tours, it wasn't like that at all. We had to walk round a massive city trying to find individual shops in the middle of random shops. So it was actually really difficult to find these places, so when we saw him and he was really friendly, yeah, you're straight away drawn to him." (P3, lines 108-120)

These excerpts demonstrate that, in order for a scammer to be taken seriously and reduce suspicion, they must embody the characteristics that a genuine provider of a service would possess. When the perpetrator of a scam is able to projects competence, through smart attire or being well-spoken, fraudulent attempts are more likely to succeed.

3.3.2.1.2 Similarity, familiarity and likeability

First impressions can also be driven by scammers giving out information about themselves and presenting themselves as being socially close to the victim, either belonging to the same community or sharing some common characteristic. This may influence a person to extend trust towards someone they have never encountered before.

In the case of Peter, who had accepted a car repair from a complete stranger, the bid to trust relied on the disclosure of personal information and especially the fact that the fraudster was 'living locally'.

> Peter: "I think he sort of put me at my ease by saying he was a mechanic and, uhm, by giving me some information about his family coz he said his daughter has just had a baby and, you know, strangers just don't do that and I think now, now thinking back I think it was

> to put me at my ease to say that, you know, I'm a good fellow who, you know, I'm a family person and I live locally and I think that was to put me at my ease really." (P3, lines 120-125)

Feeling "put at ease", to use Peter's words, is consistent with the idea that a fraud perpetrator would look different from a typical person, and especially, that they would not belong to the same social group or background as the victim.

People are more likely to trust what is familiar to them. Kate and Robin, victims of the same pyramid scam, explain that it was trusting the judgment of their friends that introduced them to the scheme that subsequently led them all to lose the funds. Knowing her friend for many years, gave Kate confidence in the venture:

> Kate: "Had it been somebody you didn't trust or I thought wasn't that bright, if I spoke to somebody I didn't know, I knew nothing about them and they went oh yeah, give me a cheque for five hundred quid, I'll give it to this person and in X amount of time you'll get some cheques for five hundred quid, I would just say no. Talking to people you trust about it, yeah it did, it's a confidence thing really." (P5, lines 231-238)

Robin further explains his trust in the judgment of his friends and the fact that the perpetrator was someone who lived and worked in the same community and was therefore considered trustworthy.

> Robin: "Uhm, some other friends were involved in it and they were involved in it by somebody they met in a quite a formal situation, it was a woman that worked in the Bang & Olufsen shop in the town where they lived, a very small town, so a small community. The woman was working in a decent shop uhm, they were good customers there and I think that gave them a sense of security in putting their money in and I kind of trusted the judgment of my friends and thought: well it may work." (P2, lines 49-55)

Kate points out how she would not have considered participating in the scheme if the proposal had not come from someone she knew. In these cases, trust is already present in the relationship so it is hard to withdraw it or question the good faith or judgment of the proponent of the opportunity.

Scammers may also cultivate interpersonal relationship with a victim in order to encourage compliance and reassure the victim. Investing a large sum of money in company shares, Henry was promised a quick return of investment. As the weeks went

by, he began feeling uneasy about the investment, as he had not received the return. After complaining, he was assigned a liaison person that would contact him daily, and who built a relatively intimate personal relationship with him. After a while, it became harder for him to complain about his investment.

> Henry: "I thought that actually if I met him I'd probably quite like him. I didn't feel the same way about the first guy who contacted me. [...] I felt sort of warmth with the other guy and a sort of sense of genuine, I mean, it felt as if he was genuinely kind of concerned to do the right thing, is what it felt like. Uhm, now whether he was much cleverer kind of manipulator of people or quite why it felt like that, it would be hard to summarise in a few words. Uhm, but the first guy I did feel that he was just a bit of a smoothie I suppose. And I didn't know anything about him personally whereas I sort of, somehow, even if it was delusionary, I felt as if I did know something about the other guy." (P5, lines 233-235 and P7, lines 332-339)

3.3.2.1.3 Limited availability

Scammers exploit a scarcity of goods, or manipulate the perception of scarcity by limiting the time their offer is valid for, thus putting the potential victim in the position where they might miss out on the purchase they aspire to make. Fred's account shows how this impacted on his decision-making. He was defrauded through an online auction site, trying to purchase a van, which fitted his needs at the time, and for a good price. He felt uneasy about a lack of communication with the seller, but did not want to miss a good opportunity.

> Fred: "Well we were very excited, initially we were very excited that, what he was offering because it was exactly what we were looking for uhm, and it was within our budget as well. Initially yeah, we were very excited about it and then an excitement probably took us over a wee bit. However, I did have a little bit of concern over the emails, uhm and I asked them numerous times to uhm, for a contact phone number so I can call them up and discuss the van and further details. They said they were out of the country, that they were err, not contactable till next week, however next week it was gonna be sold so, uhm, it was gonna have to be now or never." (P4, lines 149-157)

Offering goods at a convenient price and limiting the time the offer is presented for, can push buyers towards completion, as they may have already emotionally committed to the offer. Giving up at that point would mean renouncing the opportunity, creating a lack of closure and mean that more time resource would be needed to start the search afresh for a similar opportunity.

3.3.2.2 Factors pertaining to the victim

Regardless of the actions of the perpetrator, once a person finds a fraudulent offer enticing, different personal attributes of the victim can facilitate whether they decide to comply with or reject the scam. Two factors identified in the narratives of scam victims are discussed below.

3.3.2.2.1 Lack of scrutiny of available information

The amount of information different people gather about a product or service provider and the opportunities they present varies. In the present sample, the amount of preliminary investigation participants performed did not seem related to the amount of money they were going to invest, with some interviewees admitting to having skipped even the basic checks, as Jane explains:

> Jane: "Of course people don't, I mean, I'm sure that I'm not alone. Do you read your terms and conditions when you pay anything online, uhm, you know. Or when you buy something from Amazon, twenty pages long? Of course, you don't. Of course, you should. I'm a lawyer's daughter and when I first signed my first bank account, I absolutely read terms and conditions and showed it to my father but do I do it now? No."
>
> Interviewer: "Is there a reason for that?"
>
> Jane: "Time." (P5, lines 213-222)

While regretting not having read the small print on the website, Jane feels confident in describing her conduct as typical. She points to something scams clearly rely on, namely that routine dealings with Internet companies have socialised web users to trust providers without reading through terms and conditions. This acquired trust is exploited by scammers who count on a number of customers completing a procedure without questioning its legitimacy, especially when there is an additional urgency factor at play.

The interplay of urgency, scarcity and lack of scrutiny can also be observed in Chloe's story. The last amongst her friends to buy tickets for a music festival that appeared sold out, she used a link to a ticket website sent by one of her friends (who purchased tickets elsewhere), without checking the website's legitimacy.

Interviewer: "What do you think might have helped you to avoid it?"

Chloe: "Taking my time. To actually research a company, which I do now with any kind of transactions I do online but it did put me off buying anything online for at least four years." (P7, lines 321-325)

3.3.2.2.2 Excitement

While some transactions have to do with completing an undesirable task or getting something out of the way quickly, other fraudulent opportunities can involve the anticipation of positive emotional prospects such as securing goods, money or even a new job. Such prospects elicit optimistic images of possible futures in which such things have been obtained. Our participants recall the insurgence of feelings concerning similar promised events.

Kate: "I mean, gosh, can you imagine it, if a few people would send you a cheque for a thousand pounds each or even five hundred quid each, you know what I mean, that would be like such a nice bonus and you do kinda think ooh if I got a bonus of few thousand pounds I could go out and treat myself, I could have a holiday or I could buy myself something for the house, or you know what I mean, there's a certain like 'oooh', you know what I mean, yeah a niceness, what can I do, how can I improve where I am, could I have a nice holiday, could I have a nice, I don't know, TV or could I buy a new car or whatever it is. There was that kind of oooh that sounds nice, that sounds like I want to get involved." (P5, lines 206-217)

Having entertained such images makes the prospect of not "getting involved" seem like a loss, prompting further risky behaviours to resolve a fear of missing out. Henry, who invested twice in worthless shares, explains in detail below:

Henry: "Uhm...it seemed like within weeks I was gonna get money from this first one and that I'd be kicking myself if I didn't take the opportunity to get the money from the second one and it was enough money to make it, sort of, life changing situation." (P8, lines 367-370)

In Henry's words, it was the anticipation of regretting a missed opportunity that wins him over, after having envisioned a different life for himself. Exercising caution would make that image vanish, and this is how such future scenarios act in favour of the scammer and create a facilitated route to persuasion.

3.3.2.2.3 Social norms

Social norms such as being polite or helpful can elicit compliance in certain situations, even when there are no external pressures to comply with a request. In the excerpt below, Greg explains why saying no makes him uncomfortable.

> Interviewer: "What would be the reason that you can't just say to somebody 'I'll think about it', and walk out of the shop?"
>
> Greg: "I'm stupid. For me it's all about being polite. So I think it's rude to. So I often say oh great, I really like it, I'll come back, I'll just go get some money or need to check with, uhm, friend who is buying it as well. It's really silly and my friends often say to me it's really fake, uhm, to do that. For me it's really rude to just say no to someone." (P8, lines 348-352)

3.3.3 Aftermath

Victims of fraud are greatly affected by their experience and these feelings can be extensive and long lasting. This section illustrates the most common reactions after the event has been realised as a scam.

3.3.3.1 Psychological and financial consequences

Some participants endured a significant financial loss, which had repercussions on their subsequent life situation. However, most participants reported lingering feelings of anger and resentment against the perpetrator even when little or no money was lost.

Nina lost money buying hair styling tools online from a fake website. Paying by PayPal, she believed she would have fraud protection, but found she was not covered as the scammer persuaded her to cancel the complaint. Later, she found out that this is a frequent scamming technique, which made her angry at PayPal for not eradicating the loophole.

> Nina: "I suspect that most people feel pretty angry when they've been scammed. So, I mean that's a normal response, I'm just surprised that I still feel as much as I do so far down the line, when really at the end of the day, it's a long time ago. Actually, it's three years ago. [...] So I guess, yeah, when somebody really pisses you off, it stays with you." (P8, lines 358-363)

Other participants also expressed their ever-lasting desire for revenge against the scammer.

> Bill: "I still bring it up in my memory, I still have fantasies about getting justice somehow and being like Bruce Willis, chase him down and giving him a smack [laughs]. But I guess that doesn't go away [laughs]." (P7, lines 318-320)

Most participants also reported negative emotions directed towards themselves such as feelings of humiliation and shame, which prevented them from telling others about their experience. Additionally, some participants expressed strong self-judgments such as being gullible, greedy, or inattentive. Henry recalls the impact the scam had on his self-perception:

> Henry: "I didn't like the person that had done all this, I didn't like that aspect of my personality which was being greedy enough to kind of go and try and get this money for very little effort on my behalf. I didn't like the fact that I was greedy enough to allow myself to be persuaded, or gullible enough, to allow myself to be persuaded to spend another 20 thousand, which I didn't have. Particularly didn't like that. Uhm, I didn't like my own gullibility [...] I suppose a sense of greed and gullibility combined were aspects of myself that I didn't, uhm, enjoy coming to terms with I suppose." (P9, lines 437-444)

For Henry, the financial consequences were also considerable, and had an impact on the future.

> Henry: "In some ways it was quite life changing on all sorts of levels coz the money that I spent, I then couldn't afford to maintain the house that I had and I ended up selling that house that I had at the time that I shouldn't really have sold it. And you know, in a way they were a life changing amounts of money involved and so my life hasn't perhaps got the access to the funds that I might have had, had that not have happened." (P10, lines 483-489)

Even when no funds are lost, being deceived can have a profound effect on self-esteem. Even though Greg realised he was about to be defrauded before he lost any money, he describes being angry at himself for believing the scammer at the time.

> Greg: "I was so annoyed at myself for being caught up in that moment, ridiculously annoyed [...] I, like, when we left that room, we shook his hand and I was like; thank you so much for booking me this hotel and it really still annoys me to this day, I get bitter about it coz I shook his hand, coz I thought he was a nice person. And he was just lying, completely." (P7, lines 308-325)

3.3.3.2 Avoidance strategies

The experience of fraud leads victims to implement a variety of avoidance strategies to protect themselves from similar situations in the future. The most commonly adopted strategy consisted of being aware of the details of different scams in operation and their sophistication, whether online or face-to-face. Many participants in the sample reported having held a belief that becoming a scam victim would never happen to them, such that even a general awareness that scams can happen to anyone, might provide protection from victimisation. Some participants also formed strategies specific to their experience, usually concentrating on the details of the scam or scam delivery. The excerpts from Fred and Henry illustrate this. Fred requested to speak to the seller of a vehicle he was buying on the phone but was given excuses, and feels this contributed to him being defrauded.

> Fred: "So the first initial thing that I would give as advice to anybody is uhm, err, firstly, most important is to talk to someone on the phone. If you can talk to someone on the phone then you can actually find out if they are a real person or not." (P5, lines 225-228)

However, Henry, who was defrauded over the phone, reported not wanting to deal with anyone on the phone since the scam.

> Henry: "People often ring out of the blue for various reasons and I don't do any of it. So I don't do any dealings with people on the phone now. I say if you want to deal with me you've got to write to me." (P10, lines 467-469)

Observing patterns of behaviour in individuals that find themselves in a scam situation and do not succumb is vital for fraud prevention. Greg, who found himself under pressure to make a quick decision when booking a holiday tour, recognised it was a scam due to a strategy that he now routinely implements when in doubt:

> Greg: "Luckily for us, before we book the trip, we always go quickly check it on the Internet, just to make sure. My excuse is always 'oh just need to go get some money'. [...] So we went to get the money, but really we were going to the Internet café. […] And when we went on there, we found out that he's a scam artist, everything he promises he doesn't deliver." (P2, lines 54-69)

Greg also explained that he routinely uses the excuse of not having the money to purchase something because he is uncomfortable saying no.

Greg: “For me it is polite and it is not because you’re lying but I don’t like being rude in the shop and saying I don’t want it. So I think it’s always been a strategy in England as well but I used it a lot more in South America.”

Interviewer: “So this is a strategy to get out of an uncomfortable situation where you’re not sure about your decision?”

Greg: “Yeah.” (P6, lines 258-266)

3.3.3.3 Resolution and justice

The psychological discomfort that victims of fraud experience is exacerbated by the perceived lack of response from the authorities. None of the participants who reported being scammed to the authorities reported having their case followed up, despite some being extremely persistent and even tracking down the scammer’s whereabouts.

3.3.3.3.1 Dealing with the authorities

When a victim attempts to report fraud to The Police, they are directed to Action Fraud, an agency that records details of the fraud and passes them on to the police. Participants that reported to Action Fraud had believed the crime would be investigated or followed up, but discovered this was not the case. The excerpts below illustrate the type of reaction the lack of clear personal outcomes can engender. Fred was encouraged by Action Fraud's social media representative to call and report the fraud. When he did, he was told during the call that nothing will be done about it, despite him paying by bank transfer, through which the scammers details would be easily available to the police. This led him to erroneously believe that Action Fraud received funding per report they record.

Interviewer: "Could I ask you about Action Fraud? You mentioned that they get paid by the police for each case that they raise."

Fred: "Yeah."

Interviewer: "How did you find that out?"

Fred: "I don’t know that. I’m assuming that. The reason why I’m assuming that, because they made it very easy for me to raise the case and they made it very easy and pushed me raising the

> case but yet as soon as the case is raised, uhm, they didn't wanna hear anything about it." (P6, lines 284-294)

Rob reported similar negative views of dealing with the organisation:

> Rob: [...] "the state hasn't lost money and the banks haven't lost money, so they need to put in place a system that makes it look like ordinary people have protection against fraud. Uhm, whereas, in fact they're prepared to do nothing at all about it. The purpose of Action Fraud, uhm, is to create a barrier between police and ordinary people trying to report fraud. So they can, police can give plausible deniability that they are there to fight against fraud but actually they put this obstruction in the way." (P5, lines 242-248)

Both experiences reflect that a lack of interest from the authorities generates a very cynical response in the victim, perpetuating negative feelings after the incident and leading to broad assumptions or conspiracy theories about the operation of the organisation. In many ways, the lack of perceived interest from the authorities and their inability or unwillingness to investigate and prosecute fraud crimes redoubles the offence for the victims, who find themselves unable to let go and give the experience closure. (Rob's reporting path is outlined in Appendix 1.3, Table 1.4)

Participants who did not report fraud to the authorities, reported being too embarrassed to report it or chose not to report it because they expected nothing would be done about it.

> Peter: "I just didn't feel that I wanted to get involved with the police in that way and really, are they gonna do anything about it? They're just gonna write it in the book or give me a number, that's it. They're not gonna be able to find the person or, they're not gonna be interested in that kinda thing. That's their job, that's what they should do uhm, but I think this is termed low level crime and it's not really, not worth investigating. So really, is it worth my time to even report it?" (P4, 172-181)

3.3.3.3.2 Need for resolution

The need for support and a resolution of some kind was mentioned by all participants that reported the fraud to the authorities. The need for resolution and achievement of closure was important, even when no loss had occurred. Greg, who was fortunate enough to have avoided the scam, encountered the scammer again by coincidence and

helped stop potential victims from being scammed by him. He explains, below, that this gave him a sense of justice.

> Greg: "Because you can tell people about what happened and they go; oh that's really bad but to see him again, for me, meant everything. I got closure from that. Because I got to let everything out that has been building up and it was only, how many weeks since we've seen him? Maybe two weeks maybe three weeks, I'm not too sure, maybe two weeks since we've seen him but to get it all out was good for me and I think it helped a lot. [...] And I know I keep going on about it but it was, for me, just perfect. It was like you can't get away with things like that, it's not fair. And I think that's the thing, it's not fair what he tried to do to us. I would never do that to somebody else. And I don't understand how anyone could do that to somebody."
>
> Interviewer: "Would you say you got, like a sense of justice from it?"
>
> Greg: "Yeah, definitely. Completely, hundred per cent justice. It was like; You aren't doing this, I know he's gonna do it to other people but, you're not doing it to these people."
> (P11, lines 496-530)

Greg's words display the importance of having a second chance to engage with the perpetrator. In his case it was through a chance meeting, but for other interviewees a successful prosecution would achieve a similar sense of justice. The experience reveals many features that were common to participants, such as the reiterative nature of the thoughts about the scam, the acute sense of injustice attributed to exploiting people's trust, and the desire to prevent fraud from happening again.

3.3.3.4 Loss of trust

One of the most important repercussions of fraud victimisation reported by participants was the loss of trust that went beyond its immediate circumstances. This concerns the kind of 'systemic' trust enabling social actors to carry out their everyday business (Luhmann, 1979, 2000). From this perspective, trust is granted to fellow citizens as well as to authorities, and contributes to the sense of personal safety and order in the world. It is this breach of systemic trust that may explain the depth and duration of negative emotions experienced by scam victims, directed both outwards and inwards. Participants in the study reported a variety of enduring changes in their attitudes, from increased cynicism in evaluating other people's claims, to avoiding using certain commercial facilities and a heightened sense of threat and lack of protection.

> Peter: "It's quite sad, it's sad because there are genuine people out there that do need help, even if it's just a bit of advice. Even if somebody approaches me and says do you know this road and how to get there, uhm, nine times out of ten yes do know but I'll even say to them sorry I'm very busy, I need to go. Don't even bother to stop and talk." (P7, lines 299-303)

> Nina: "Uhm, it has stopped me ordering from small, unknown companies because I just don't trust them anymore. [...] It's a shame, you know. There could be some amazing small company out there that does an incredible product and I would never ever order off the Internet off them now." (P6, lines 246-253)

Peter's and Nina's accounts points to a sense of estrangement and indifference to others resulting from his experience with a scammer; Rob similarly mentions both a change of attitude towards others and the authorities:

> Rob: "I learnt some things about human nature and I've had my suspicions about the government reinforced. Uhm, there is no protection, you're on your own, if you send money somewhere by accident, you'll never get it back." (P13, lines 593-595)

Rob's words, and especially the phrase "you're on your own" encapsulated the feelings of several interviewees upon discovering that the blanket of legal protection we assume extending over us is a lot smaller than they had previously imagined.

3.4 Interview study Discussion: Study 1

The study reported in this chapter set out to illuminate the full process of fraudulent action, in order to gain a new perspective and deeper understanding of the circumstances that influence the initiation, cooperation, and consequences of fraud victimisation. Exploring scam events through narrative accounts has helped identify the different elements required for a scam to be successful across its different stages. Three stages of the scam process, from the victim's perspective, were identified; circumstances leading to engagement with fraudulent offers, factors implicated in continuous engagement and the aftermath of fraud, in which different elements operated, alone or in combination. The findings supported previous research outlining factors that may influence compliance with fraudulent offers, such as trusting individuals that appear credible, friendly or familiar, feeling excited at the prospect of

attaining the scam offer or trusting legitimate looking scam communication (Langenderfer & Shimp, 2001; Lea et al., 2009; Whitty, 2013).

Several types of scams are based on casting a 'net' out, via an offer that looks presentable enough for a number of people to be persuaded of its value. These often entail limited engagement due to time or the scarcity of goods; they can be online or face-to-face but transactions are typically characterised by relatively few exchanges. In many cases the credible presentation of offer material, a scammer's presentable demeanour and the strategies they use to avoid arousing suspicion, generate trust that things are what they look like. This type of trust promotes cooperation given its foundation in everyday life. For example, each time we purchase goods online, we trust that a vendor will fulfil their end of the bargain and deliver the purchase (Luhman, 2000; Misztal, 2013). Crucially, participants who were victims of scams related to purchasing services or goods, reported that it may have helped them personally to be more aware of the reality of potential deception.

Trusting intermediaries, either because they were part of an existing social network or because they were able to present themselves as similar to the victim was key, as it made people dismiss their doubts sufficiently to let the potential positive outcomes of the opportunity exert their attraction. A strong pull factor for some victims was the promise of getting richer and the imagined positive scenarios this creates, especially when the current circumstances of the person were problematic. For others, the experience simulated ordinary situations, such as making purchases online, often without visceral triggers present.

The level of emotional distress and anger experienced in the aftermath of a fraud is not always connected to the amount lost; rather, it seems related to the fact of the deception itself and the level of trust that the person had accorded to the scammer. This suggests that fraud may be extremely harmful to some victims, even when the amount is low or no funds are lost. Finding a resolution and experiencing a feeling of justice following fraud victimisation seems to be an important part of the healing process (Button et al., 2015), alleviating the recurrent feelings of anger and self-blame experienced by many victims. However, reporting the fraud can, within current mechanisms, add to the hurt and frustration victims feel, prolonging the psychological distress after victimization.

3.4.1 Individual risk factors in fraud vulnerability

The aim of the present study was to identify the main personal attributes that may be contributing to scam compliance. Looking at the interview data through the lens of the human response to events was important, in order to generate questionnaire items for a measure developed in Study 2 (Chapter 4). The present study explored reflections on the experience, identifying factors that may protect one from fraud victimisation. Whilst the interviews have identified several commonalities in the events and techniques used in scams in accordance with previous research, evaluation of these commonalities has tried to go beyond these basic features to examine the human attributes that may be connected in the interpretation of these events. Being in a hurry or not having the time to consider all the information led to rushed decisions or decisions based on insufficient information, while being excited at the prospect of a scam offer reduced motivation to scrutinise finer details. Encountering someone who appeared likeable and friendly elicited trust and compliance, as did investments and schemes that had a backing of those from the same peer group. Certain personal circumstances that affected the emotional state of the participant, (e.g. being unhappy in a current job), influenced the dismissal of the warning signs and led to decisions, which were out of character and later regretted. A desire to attain goods or services that appeared to be scarce, or their availability was limited, lead to riskier choices and less caution and being pressured to make a decision quickly led to compliance. Personal attributes that emerged from the findings were organised around the themes, in order to inform the questionnaire items. These included; trusting those that appeared similar or those that are liked, inability to say no when under pressure to comply, rushing decisions when confronted with lack of time to consider information, making risky choices when confronted with difficult personal circumstances etc.

The data collected and analysed in the present study informed the development of questionnaire items used in the construction of the Susceptibility to Fraud Scale, a measure used in the consequent studies in this programme of research. For example, themes identified in the present study were used to develop questions pertaining to liking and similarity, urgency, compliance, vigilance, rushing decisions or impulsivity. Questionnaire item development is not discussed at length in this chapter, as it forms a part of the consequent study, Study 2. Further information on how the data from Study 1 informed the questionnaire development in Study 2 can be found in the following chapter, Chapter 4, with examples presented in Table 4.1.

3.4.2 Reflexivity

Reflexivity refers to the influence that the researcher may have on the participant as well as data collection (e.g. prior knowledge of the participant). It also applies to analysis (Burman, 1994). For example, it may affect which quotes are chosen when presenting results. Therefore it is important to consider the position of the researcher/author when reading the findings of a qualitative study.

The author is a middle aged, Caucasian woman of Eastern European ancestry (Croatia) and is a long term UK resident. With a background in psychology, she has never worked with victims of fraud or as a fraud prevention professional and participants were made aware of this. As a result of this, participants may have felt more comfortable discussing shortcomings of the UK based fraud prevention and reporting organisations, as several participants reported dissatisfaction with reporting fraud to the authorities. However, as someone who has never been defrauded and without the experience of dealing with fraud prevention and fraud reporting organisations, the author is likely to view the issue of fraud victimisation from an outsider's perspective. This perspective may have reduced the bias connected to reporting of the results, as it affords a position of neutrality, especially with regards to fraud victims that expressed dissatisfaction with fraud reporting agencies, but is also worthy of consideration. As someone who has never experienced fraud victimisation and the psychological effects this may cause, the author may have unintentionally misrepresented the experiences of the participants in this study or omitted the data that a victim of fraud may deem significant.

Additionally, in terms of data collection for the present study, there are several considerations to note:

(i) One of the participants was known to the researcher prior to the interview and volunteered to participate when the matter of the research was discussed in a casual conversation.

(ii) One of the participants, who volunteered to participate in the study, discussed the study with his friends, following participation. This resulted in a friend who was defrauded with him to contact the researcher and volunteer to participate. The same person also told another friend, who, as a result contacted the researcher and volunteered to participate in the study. Although participation was voluntary and the participants contacted the researcher asking

to participate, there is a chance that the first participant encouraged his friends to take part.

(iii) One interview was emotionally difficult to conduct for the researcher, due to the fact that the victim was greatly affected by the scam and was distressed at one point during the interview, asking for a pause, which was provided. It was clear, upon return that the participant cried while away from the interview. At the end of the interview, the participant was encouraged to discuss if anything could be improved to minimise hurt, if the researcher could have been more sensitive or could have done anything differently but reported that there was nothing that could have been improved. It is possible that the emotional response evoked by this interview affected the researcher's motives for selection of material presented in this study.

3.5 Future considerations and implications

The findings of the present study indicated that there may be differences in how different people process and experience fraudulent offers, as well as other individual vulnerabilities, such as personal circumstances that may make a scam offer more attractive. Given a certain amount of credibility, many participants decided to go along with the scam, despite not having gathered enough information or feeling uneasy about it, where others might have exerted more caution and investigated further. By interviewing two participants that were engaged in the same pyramid scheme, two different perspectives on the same fraud were observed. Participants had different recollections on what information was relayed to them at the time and what they thought this information meant. They also reported different reasons for complying with the scam when asked, illustrating the fact that motivations to engage with the scam as well as factors that prove influential for successful persuasions are not the same for all people. These cases illustrated that despite detecting something wrong, individuals can go along with the scam for personal reasons that have little to do with the scam (i.e. to be part of the group that is also engaging with the scam). Future studies may want to look into differences in the interpretations of the same fraudulent information.

One of the limitations of this study is the self-selection bias. Apart from the exclusions based on the recruitment criteria, all the participants that responded to the study and wanted to participate and were interviewed until the data saturation was reached. The study did not use any intermediaries for recruitment (e.g. organisations that work with fraud victims), therefore only those participants that contacted the researcher directly and wanted to talk about their experience were selected. This may mean that other, more reticent fraud victims were not represented in this study. Another limitation was the inability to recruit more participants that came close to losing funds to fraud but perhaps realised on time, in order to examine techniques and strategies used by such individuals.

Although the interviews with victims of fraud yielded quality data, it would have been of value to interview more participants that came close to being defrauded but realised it was a scam before being defrauded, as the interview with one participant fitting this description provided an insight that some people may be aware of specific weaknesses that may make them more susceptible to fraud and how they compensate for it. As soon as this was noted, recruitment concentrated on finding participants who came close to being defrauded but realised before losing funds, however, it proved very hard to recruit participants fitting this description. One reason for this may be that victims of fraud felt they were not taken seriously by the authorities or they were too ashamed to talk to people they know about their experience, and were therefore more motivated to share their experience than those who avoided fraud victimisation and were not affected by it as much. For example, Schiebe et al. (2014) found a positive association between falling for the scam they simulated in their study, and a willingness to complete a follow up survey. However, these findings may be a key to developing new strategies for fraud prevention, specifically making people aware of their own areas of vulnerability and designing specific measures or advice to address these vulnerabilities. Future studies may want to focus on interviewing participants that came close to being defrauded but realised in time, in order to examine if this was down to specific awareness of individual characteristics they possess that would make them more vulnerable in certain fraudulent situations.

Fraud victimisation leads to a loss of confidence and trust in authorities, which may result in a lack of fraud reporting and cooperation with authorities in the future. In addition, loss of trust may alter people's attitudes towards others, therefore creating

longer-term consequences of fraud victimisation in society, which could be potentially devastating and have a serious impact on the victims' interpersonal relationships. The sheer amount of fraud perpetrated nowadays means that the financial burden on the authorities to investigate every fraud reported is immense and unrealistic. However, an honest and more sympathetic way of addressing victims of fraud is needed and may be achievable by being more transparent about how complaints are processed. Even a small token of empathy may be extremely therapeutic for victims of fraud.

Finally, the majority of participants reported they 'learned their lesson' and modified their behaviour following the scam, but sometimes these modifications or coping mechanisms only addressed the way scam was delivered (e.g. avoiding the internet or the phone), and may still leave them open to future fraud victimisation via other delivery methods. Therefore, organisations may benefit from developing individually tailored analysis of users' weak points, in order to design more applicable prevention advice, as it is clear that once defrauded, most people try to prevent future victimisation.

3.6 Conclusion

The present study explored, through the narratives of fraud victims, processes that underlie fraud victimisation, in order to reveal individual attributes implicated in vulnerability to fraud. The study identified three distinct stages of the scam process from the perspective of the victim; precursors to the scam, which may enhance the attractiveness of the scam offer, commitment stage, in which different factors combine to enhance compliance and the aftermath, incorporating processes that often follow fraud victimisation. These include; reporting fraud and trying to attain a resolution, dealing with psychological or financial consequences and incorporating behavioural changes in order to avoid future victimisation.

Several individual attributes that appeared to contribute to fraud victimisation were identified; rushing decisions when under pressure to make a decision or when time is of the essence, complying with requests due to social norms, taking risks to attain desired products or services etc. The present study identified individual attributes and adapted behaviours that may help protect from future victimisation. These included forming strategies to compensate for individual fraud vulnerabilities, such as delaying decisions,

careful information processing or even lying to get out of potentially harmful situations. The present study also found that while most people develop these strategies after they are defrauded, some people are aware of their personality attributes irrespective of victimisation, which predisposition them to being defrauded in certain situations, and try to compensate for them.

The personal reasons and motivation for engaging with fraudulent offers, differ between people that find themselves in the same fraudulent situation. Fraud techniques, social mechanisms and other situational factors or life events, as well as individual attributes, may contribute, in various degrees, to fraud victimisation, making the process unique to each individual. As scammers frequently adapt their techniques and scam narratives, concentrating on warnings that address specific individual vulnerabilities with regards to fraudulent offers and situations, may be a better way of forewarning and educating about dangers of fraud.

Chapter 4

Predicting individual differences in vulnerability to fraud: the development of a Susceptibility to Fraud scale

4.1 Introduction

This study builds on research conducted in Study 1, interviews with victims of fraud (see Chapter 3). It is also informed by research conducted by Lea et al. (2009) and Modic and Lea (2012, 2013), which explored susceptibility to persuasion and errors in judgments. Models of Gullible and Foolish Action by Greenspan (2008, 2009) and a Model of Scamming Vulnerability by Langenderfer and Shimp (2001) were taken into consideration and informed the development of the initial questionnaire items. The same is true for studies addressing trust and vigilance (e.g. Markóczy, 2003).

The first stage of the scam experience identified certain components, or precursors, that make responding to the scam more likely, while the second stage identified factors pertaining to the scammer (e.g. different techniques used) and those pertaining to the victim (e.g. emotional reactions to fraud offers). These findings informed the development of the initial item pool used in the construction of the Susceptibility to Fraud Scale, and specifically, questions pertaining to liking and similarity, urgency, insufficient information processing, social norms that govern compliance and trusting legitimate and credible looking scam offers. Urgency, imposed by the time constraints (external event), related to rushing decisions or insufficient information processing, while urgency (imposed by the scammer) related to compliance. Liking and similarity related to compliance with requests by those that appeared likeable or similar in some way. The examples of how the data from Study 1 informed the questionnaire development, are presented in Table 4.1.

In addition, emotional states and visceral reactions that the fraud offers evoked in some participants. Participants' reflections on the experience and what they would do differently if they were in the same situation, informed the construction of items concerning the time allowed for decision-making as well as items pertaining to vigilance. Many participants were surprised at the lack of interest from the authorities, following the scam, and these findings informed the construction of items that pertain to belief in justice and protection from crime. This may be explained in the context of just world hypothesis (Learner 1965). Just world hypothesis states that: "people have a need to believe that their environment is a just and orderly place where people usually get what they deserve" (Lerner & Miller, 1978, p.1030).

Table 4.1

Examples of questionnaire item development using the data from Study 1

Unit of meaning	**Theme/ Subtheme**	**Questionnaire item(s)**
"Friendly and genuine, uhm, that's pretty much it, non-threatening. [...] I guess it made me think of someone I can relate to..."	Similarity, familiarity and likeability	I find it hard to say no to people I like.
"So, there must've been something that wasn't quite right and I think it was the pressure, coz he was really really putting pressure on us to book it straight away."	Urgency	I am always suspicious of people who ask me to make quick decisions.
"Uhm, and I, yeah just do my research and buy from reputable uhm you know, websites and companies. And ask my friends have they bought from there as well."	Credibility and legitimacy	I am always careful to check out people and companies if I haven't bought from them before.
"I: So why do you think you didn't read terms and conditions? R: Just a really really busy time at work. Doing 12 hour days."	Time constraints	I prefer to take my time to think things through.
"You see, unfortunately, the way I was feeling on Monday, have I seen it I probably would have still gone ahead with it, coz sometimes you're feeling desperate, d'you understand what I mean, you don't think to think so clearly."	Dissatisfaction with one's present circumstances	When I find myself in a difficult situation I often make decisions I later regret.
"For me it's all about being polite. [...] For me it's really rude to just say no to someone."	Social norms	I find it hard to say no to people without seeming rude.

Giving an illusion that one can control one's environment, belief in just world is an important adaptive function, without which the pursuit of long-term goals and behaviour regulation may be hindered (Lerner & Miller, 1978). Belief in just world may also be beneficial to mental health, by maintaining self-esteem and general wellbeing and contributing to life satisfaction (Dalbert, 1998, 1999).

Lea et al. (2009) suggests that scam victims have a general vulnerability to persuasion and not a specific weakness towards the type of scam offer they responded to. Research looking at individual factors that may govern scam compliance has demonstrated that

the development of purpose made measures may be essential in pinpointing individual vulnerability to fraudulent offers (Fischer et al., 2013; Modic & Lea, 2012, 2013).

4.1.1 Errors in judgments

Lea et al. (2009) conducted a series of large-scale studies, including victims of fraud as well as their family members, examining considerable amount of scam correspondence, gathering information on attitudes and behaviours via questionnaires as well as simulating a scam offer in order to capture individual's responses at the time the scam offer is evaluated. Based on their findings, Lea et al. (2009) identified motivational and cognitive factors involved in errors of judgment connected to scams. A summary of these factors can be found in Table 2.3 in Chapter 2.

Motivational factors include visceral influence, reduced motivation for information processing, preference for confirmation, lack of self-control, liking and similarity, sensation seeking, reciprocation, mood regulation and commitment and consistency. Cognitive factors included reduced cognitive abilities, positive illusions, background knowledge and overconfidence, norm activation, false consensus, authority, altercasting and social proof. There was an overlap between the findings from the previous study, Study 1 (Chapter 3), and cognitive and motivational factors identified by Lea et al. (2009), such as liking and similarity, reduced motivation for information processing, social proof, norm activation, mood regulation and authority, suggesting that questionnaire items referring to these factors would be appropriate for the scale.

4.1.2 Gullible and foolish action

Models of Foolish action and Gullible action were proposed by Greenspan (2008, 2009) in order to explain how different factors may influence behaviour that is not in one's best interest and which often happens in the presence of manipulation by others, however, they have not, as yet been validated by experimental evidence. The models are explained in detail in Chapter 2 and can be found in Figure 2.4 and Figure 2.5 in Chapter 2. There was an overlap between the findings of the previous study (Study 1) and the Model of Gullible Action (Greenspan, 2008). For example, making decisions under the strong influence of emotion (state) was reported by some participants; employing lazy thinking and not checking the facts despite being aware it is advisable to (cognition), or being in a presence of a skilled and charismatic scammer or facing time pressures (situation). Additionally, being agreeable and trusting (personality).

Some participants reported modifying their behaviour following the victimisation such as postponing decisions, which according to Greenspan (2008) may help avoid gullible acts. These findings informed the development of questions referring to making decisions under the influence of excitement or strong desire, questions referring to information processing, making rushed or forced decisions and complying with requests of others.

4.1.3 Trust and vigilance

Langenderfer and Shimp (2001) suggested that gullibility and a trusting nature separate fraud victims from non-victims. For example, research by Workman (2008) consisted of long-term observations in a professional organisation. Questionnaires and psychometric measures as well as different simulated phishing attacks were sent to employees, in order to observe employees' vulnerability to phishing attacks. Workman (2008) found that trusting individuals were more likely to succumb to social engineering attacks, such as phishing emails or phone calls. Fischer et al. (2013) found that previous fraud victimisation was associated with the trust in the scammer.

Trust often involves accepting vulnerability, as it depends on the intentions and behaviours of others. In other words, when we extend our trust, there is a risk that others may not fulfil their responsibilities towards us (Luhman, 2000; Rousseau et al., 1998). The amount of trust extended depends on the assessment of this risk. For example, a decision-making experiment by Evans and Revelle (2008), found that when participants were asked to send and receive money with an unknown partner, they were more likely to reciprocate when told the partner has invested the same or larger amount of money than when told they did not invest as much. Therefore, trust may be instrumental in predicting others' behaviour and incidentally, be connected to vulnerability to fraudulent practices and one would presume that more trusting individuals would be more vulnerable to scams. However, research by Yamagishi and Kakiuchi (2000) used the prisoner's dilemma game to examine if trusting individuals would be able to predict the behaviour of the opponent. They found that participants higher on a trust measure were better at predicting the behaviour of their opponent than participants that were less trusting, and argued that this shows that being trusting does not necessarily mean one is gullible.

In the study by Markóczy (2003), participants were given trust and vigilance scales and asked to predict the behaviour of others, related to current events (e.g. electricity shortages). She found that people high on trust differ in the amount of vigilance they possess and that prudent trusters (high in trust and high in vigilance) were better at correctly predicting others' behaviour. Vigilance may, therefore, be important factor implicated in accurate predictions of others' behaviour, something that might be beneficial in spotting fraudulent offers.

The research shows that there may be a connection with fraud victimisation and trust (Fischer et al., 2013; Langenderfer & Shimp, 2001; Workman, 2008) but that this may be moderated by the amount of vigilance one possesses (Markóczy, 2003). However, vigilance has not been empirically considered with regards to vulnerability to fraud yet the findings from the previous study, interviews with victims of fraud (Chapter 3), pointed to the fact that fraud victims become more vigilant following the victimisation. This manifested itself in being generally more aware of what others may do and what their intentions may be. Therefore, questions pertaining to trusting nature as well as questioning the motives of others were included in the questionnaire development.

4.1.4 Model of scamming vulnerability

Langenderfer and Shimp's (2001) theoretical Model of Scamming Vulnerability explains how the attention is directed under high and low visceral influence. Visceral influence takes our attention away from the usual information processing (i.e. when hungry and in presence of food, people find it hard to concentrate on anything else). Scammers often exploit visceral influences such as greed (high-return investments, fake lotteries) or sexual desires (romance scams), therefore better understanding of the factors that moderate visceral influence is vital for fraud prevention. The model is found in Figure 2.3 in Chapter 2.

Langenderfer and Shimp (2001) suggest that the attention people pay to the fraudulent messages can be considered in the context of Elaboration Likelihood Model (ELM) of persuasion (Petty & Cacioppo, 1986). ELM identifies two routes of information processing; peripheral and central. The peripheral route utilizes little elaboration and relies on persuasive cues while central route concentrates on the message arguments. The model can be found in Figure 2.7 in Chapter 2.

Scammers frequently evoke visceral influence in order to bypass the central route of processing and instead, get the potential victim to focus on scam reward instead of the

scam information, which may alert to potential danger. Langenderfer and Shimp (2001) suggest that there are certain factors that moderate, as well as influence scam vulnerability under the low and high visceral influence. Self-control is identified as the only factor able to prevent scamming vulnerability under high visceral influence. Even under the low visceral influence, there are certain factors that increase scam vulnerability, such as cognitive impairment, social isolation, consumer susceptibility to interpersonal influence and gullibility, while scepticism and scam knowledge act as moderators.

Langenderfer and Shimp's (2001) Model of Scamming Vulnerability is yet to be tested and validated. The Model of Scamming Vulnerability was based on the data from the research conducted by the American Association of Retired People and by interviewing professionals from Better Business Bureau, an organisation promoting ethical conduct for elderly people. This means that the data used to construct the theoretical model of scamming vulnerability may not be as applicable to wider populations (e.g. elderly people frequently suffer cognitive decline, whereas this is not common in younger people). However, it is a starting point in trying to identify components responsible for scam compliance, therefore, the moderators of scamming vulnerability were taken into consideration when designing the STFS questionnaire items.

4.1.5 Susceptibility to persuasion

Modic and Lea (2012, 2013) conducted a series of studies looking into susceptibility to persuasion and scam compliance. In one of the studies they found that individuals who are more extroverted, better at predicting scam outcomes and less agreeable are also less likely to respond to scam offers (Modic & Lea, 2012). In the consequent studies, Modic and Lea (2013) constructed Susceptibility to Persuasion (StP) scale, which yielded four reliable factors of scam compliance; low self-control (e.g. difficulty controlling impulses), authority (e.g. trust in authority figures), consistency (e.g. strong need for consistency and structure) and social influence (e.g. peer or social circle influence). Although Modic and Lea (2013) developed a valid scale that pinpoints susceptibility to persuasion, their study design had some limitations, such as a small number of people reporting they have lost money to the scenarios presented to them. Due to this, scam compliance was measured in terms of responding to the scam offer rather than losing money to the offer. However, some scenarios, such as a classified advert or an auction scam do not differ from genuine adverts until the communication

with the seller is established, therefore people may respond initially but withhold funds once there are warning signs. As such, responding to some fraudulent offers may not be a good indication of scam compliance. Additionally, scam compliance was not measured in the given moment but rather by asking participants if they responded to fraudulent offers similar to hypothetical scenarios in the past three years (also Modic & Lea, 2012). Nevertheless, Modic and Lea (2012, 2013) studies offer a new way of looking at compliance with fraudulent offers, by concentrating on individual attributes, which may increase the likelihood of falling for a scam. The present study aimed to address the limitations of Modic and Lea (2012, 2013) studies by giving participants examples of genuine and phishing email correspondence from the same company and asking them to decide if the correspondence is real or fake, measuring scam compliance in the given moment.

There was an overlap between the findings from Modic and Lea's (2012, 2013) studies and the interview study with fraud victims (Chapter 3), with regards to trusting authority figures, social influence and low self-control. Given this fact and since Susceptibility to Persuasion scale is the only measure that has been successfully used to measure responding to scams, it was deemed to be an appropriate measure of concurrent validity for the measure being developed in the present study.

4.1.6 Research aims and rationale

The aim of the present study is to build on research by Modic and Lea (2013), in order to develop a measure of susceptibility to fraud.

The broad aims of this study are:

- To generate a pool of questionnaire items consulting the data from Study 1 (Chapter 3) and the available fraud research, models and theories relating to vulnerability to fraud
- To distribute preliminary questionnaire items to fraud experts, researchers in the field, fraud victims and non-victims, for consideration, in order to establish content validity (pilot study)
- To evaluate the newly developed measure against the examples of phishing and genuine email correspondence and hypothetical scam scenarios

- To assess the concurrent validity of the newly developed measure by comparing it against Modic and Lea's (2013) Susceptibility to Persuasion scale, measuring similar constructs

Once the initial pool of questionnaire items has been generated, they will need to be assessed for how accurate they represent vulnerability to fraudulent offers. Since the proposed measure of susceptibility to fraud needs to measure what it claims to measure, the initial pool of questionnaire items will be evaluated and rated by fraud experts (e.g. fraud police detectives and other professionals working with fraud victims) and researchers in the field, as well as previous fraud victims and non-victims. These ratings on a concept will inform the improvement of the final questionnaire items. Measuring scam compliance in a given moment has proved to be challenging without serious ethical implications. The present study aims to measure scam compliance by presenting examples of genuine and phishing correspondence to participants and asking them to decide (in the moment) if the correspondence is genuine or fake, addressing some of the limitations encountered by previous studies (e.g. Modic & Lea, 2012, 2013; Scheibe, 2015). At the same time, participants will be given the newly developed measure of fraud susceptibility, in order to explore individual attributes that may be connected to fraud vulnerability.

4.2 Pilot study

4.2.1 Questionnaire item development

An initial item pool of 56 statements was generated from available theories of gullible action and scamming vulnerability (Greenspan, 2009; Langenderfer & Shimp, 2001) and past research on the subject of vulnerability to fraud and persuasion (Lea et al., 2009; Modic & Lea, 2013), as well as the lived experiences of previous victims of fraud interviewed in the first study (Chapter 3). Table 4.2 shows the preliminary item categories used to formulate questions, question examples for each category and the key research that informed the development of the questionnaire items in that category.

Several items measuring beliefs about the justice system and the authorities were added in order to examine if people's perception of justice (i.e. that the perpetrator would be

caught and their funds would be recovered) would make them more vulnerable to scams by making them less careful.

Table 4.2
Examples of questionnaire items, relevant categories and the research informing item development

Item category	Example of the questionnaire item	Relevant research					
		1	2	3	4	5	6
Social norms	I find it hard to say no to people without seeming rude.	*			*		
Liking and similarity	I tend to believe people I feel I connect with.	*			*		
Social influence	I usually find it easy to agree with others in a group.	*			*		
Trust	I find it hard to tell if someone can be trusted.	*	*			*	
Urgency	I normally give in when people pressure me to make a decision.	*			*		
Information processing	I never bother double-checking terms and conditions.	*	*	*	*		
Vigilance	I often double-check what other people tell me.	*		*		*	
Decision making	I don't like to rush my decisions.	*	*				
Impulsivity and self-control	I feel compelled to act immediately when I see a bargain.	*		*	*		
State/ affect	I find it hard to contain my excitement when lucky things happen to me.	*	*	*	*		
Dealing with mistakes	I try hard to understand the reasons for any mistake I make.	*					
Trust in Authorities and justice	The Authorities, overall are effective at protecting us from crime.	*			*		
Views of fraud victims	Only gullible people fall for scams.	*					*

Notes.
1 = Study 1 (present thesis)
2 = Model of Gullible Action (Greenspan, 2009)
3 = Model of Scamming Vulnerability (Langenderfer & Shimp, 2001)
4 = Factors implicated in scam compliance (Lea et al., 2009; Modic & Lea, 2012, 2013)
5 = Trust and vigilance (Markóczy, 2003)
6 = Discourse around fraud victimisation (Cross, 2013, 2015)

The present research with scam victims reported in this thesis (Chapter 3) found that fraud victims believed that if they were defrauded, perpetrators would be caught and they may recoup their funds and this is supported by research by Lea et al. (2009), who

suggests that this gives an illusion of control over the situation. Additionally, two questionnaire items were generated according to research on discourse surrounding victims of fraud (Cross, 2013, 2015), specifically that victims of fraud are gullible and deserving of what happened to them. As fraud is widespread and often sophisticated, it was thought that it would be important to show if these attitudes would make one more vulnerable to scam offers (e.g. many people erroneously believe they could not be defrauded).

At the time the questionnaire was being designed, the news contained a story of a UK police commissioner discussing the issue of financial institutions automatically reimbursing victims of fraud for their losses in the news, asserting that this encourages lax security behaviour and that victims should, instead, be incentivised to protect themselves from fraud (Evans, 2016; Grierson, 2016). As this was an important topic related to fraud victimisation at the time, and given the fact that many participants in the previous study admitted not being as careful as they have been since the experience, this topic may be an indication of how safe people feel with regards to fraud and whether that would indicate less caution.

4.2.2 Participants

A total of 47 evaluators were recruited to provide feedback on the initial item pool including 21 fraud prevention experts and academics, 16 previous victims of fraud and 10 individuals who had never been defrauded. Participants from the interview study (Study1, Chapter 3) were also invited to participate. The non-victims were included in order to examine if the questionnaire items would make sense to those that have never been defrauded. The fraud prevention experts were drawn from a range of professions including forensic accountants, City of London Police detectives, cyber security advisors, Trading Standards officers, HRMC Fraud investigators as well as academics and researchers working in the field.

4.2.3 Materials and Procedure

A total of 56 questionnaire items were distributed using online survey software to all evaluators. The evaluators who were independent from the researcher, were told that the study aims to develop a measure of individual's vulnerability to fraud, and asked to rate the perceived applicability of each item as being an important factor in someone's individual vulnerability to fraud. In order to reduce the acquiescence bias, a Semantic

Differential scale was used, with importance ratings ranging from 0 = Not important to 10 = Very important, (Robson, 2011).

The content validity of each statement was assessed by considering not only the ratings given to each statement but also the open text feedback provided by the evaluators. Any questions with mean applicability ratings below 6.0 out of 10 were automatically eliminated, with further items being discounted based on feedback received. Two items were also reworded based on feedback received. A total of 45 items were carried forward for inclusion in the main survey. Mean item applicability ratings for the initial 56 -item questionnaire items and relevant feedback received are shown in Appendix 1.4 of this thesis.

4.3 Main study

4.3.1 Materials and Procedure

A total of 45 questionnaire items were distributed in the form of an online survey (Qualtrics), alongside the 12-item Susceptibility to Persuasion scale by Modic and Lea (2013), which was used to assess concurrent validity. Responses to each statement on both scales were made using a standard 5-point Likert scale (Strongly disagree to Strongly agree).

In addition, 7 (out of the 9) scam scenarios used by Modic and Lea (2012, 2013) were given to participants to consider. Participants were then asked to indicate, for each scenario, how likely is it that a scenario is a scam and how likely it is that people would react favourably to it. The responses were made using a 5-point scale (Extremely unlikely, Unlikely, Neither likely nor unlikely, Likely, Extremely likely). Participants were also asked if they had found themselves in a similar situation to that described in the last 3 years, and if so, whether they had responded to it or lost money as a result (Yes or No).

Two examples of email correspondence from the same company (Apple), one a phishing attempt and one a genuine email were used as test stimuli to represent potential scam scenarios that participants were asked to judge. The examples of email correspondence can be found in Figure 4.1. For each email correspondence scenario, again participants were asked to rate how likely it was that it was a scam and how likely

is it that people would respond favourably to it. Participants were additionally asked to decide whether they felt each email example was real or fake and to provide confidence ratings regarding their judgment certainty.

The study was approved by the university's Science Faculty Ethics Committee.

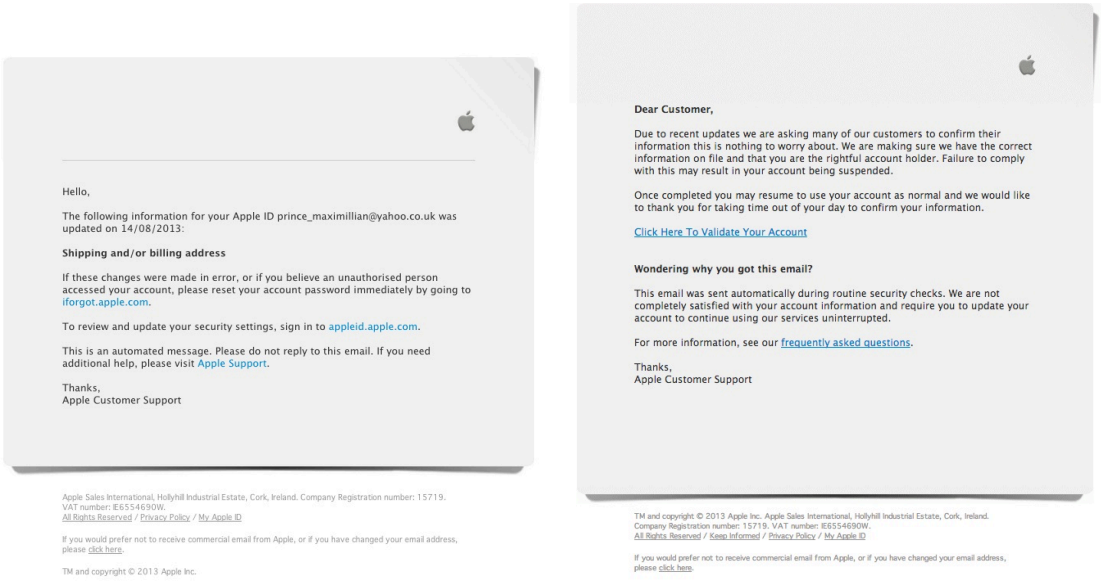


Figure 4.1 Examples of email correspondence stimuli

4.3.2 Participants

Participants were recruited via advertisements placed on open social media and via an internal participant pool scheme at the university. A total of 536 respondents completed the survey, of which 255 were university students. All participants completed the survey voluntarily and no payment was awarded for its completion. First year university students received course credits for taking part.

Responses with missing data, as well as participants taking less than 5 or more than 60 minutes to complete the survey were excluded. Participants were expected to take, on average, between 10 to 25 minutes to complete the survey in question, therefore taking too little or too much time may indicate that the participant was not taking the task seriously. Therefore, their data may not be suitable for analysis.

Further responses were excluded on the basis of unusual response patterns (response acquiescence or extreme data values on individual items where $>Z \pm 3$). This yielded a

final sample of 536 participants, aged 18 and 82 years, of whom 362 were female (*M*= 26.55 years, *SD*=12.18) and 174 were male (*M*= 33.27 years, *SD*= 16.98).

A total of 114 participants reported being defrauded once or more in the past and 422 reported they have never been defrauded.

4.3.3 Results

4.3.3.1 Results of the factor and reliability analyses

To evaluate the item structure of the 45-item questionnaire, an exploratory factor analysis using principal components extraction was conducted. Kaiser-Meyer-Olkin measure of sampling adequacy, 0.86 and Bartlett's test of sphericity (χ^2 (990) = 6572.1, p< .001) indicated that the data were suitable for factor analysis. A parallel analysis using Monte Carlo PCA indicated that only factors with a minimum Eigenvalue of above 1.59 should be retained, and inspection of the scree plot analysis suggested a point of inflection to occur in eigenvalues following the extraction of five factors, indicating a five-factor solution to be the most appropriate for these data (Pallant, 2013). Oblique rotation was used to determine factor composition. Initial item loadings for each of the five factors are shown in Table 4.3.

To strengthen the composition of each factor, 14 questions with item loadings below .45 were removed and the analysis was repeated again on the remaining 31 items. A further 4 questions with item loadings below .50 and 1 question with no clear parent factor weighting were removed leaving a final 26-item, 5 factor scale. The final version of the Susceptibility to Fraud Scale (STFS) can be found in Appendix 1.6

The first factor extracted which accounted for 16.41% of the variance in participant responses primarily related to the extent to which the respondent was inclined to go along with the wishes of others. This factor loaded most heavily on questionnaire items relating to finding it difficult to say no to people, not wishing to appear rude or agreeing to things they did not really want to. This factor was, therefore named 'Compliance' and consisted of 9 items (Cronbach's α = .87). Positive loadings on this factor may indicate a person whose thoughts or actions are more likely to accede to the will of others.

Table 4.3
Factor analysis using principal components extraction of the 45-item questionnaire

Question	Component				
	1	2	3	4	5
1. I find it hard to say no to people without seeming rude.	**.760**	.008	-.084	-.026	.075
2. I find it hard to say no to people I like.	**.748**	-.083	-.016	-.005	.010
3. I often find myself agreeing to things I don't really want to do.	**.740**	-.088	-.079	-.035	-.004
4. I normally give in when people pressure me to make a decision.	**.709**	-.007	.037	.100	-.044
5. People tell me I am easy to persuade.	**.680**	.013	.029	.014	-.087
6. I feel others often take advantage of me.	**.670**	-.024	.063	-.132	.072
7. I often worry about disappointing people.	**.613**	.126	.126	-.036	.040
8. I would prefer to be impolite rather than agree to something I don't want to do.	**-.591**	-.021	.136	.022	.242
9. When I find myself in a difficult situation I often make decisions I later regret.	**.550**	-.228	.011	-.017	.138
10. I always do what I think is best, even when I am in the minority.	**-.483**	.004	.159	.115	.325
11. I tend to believe people I feel I connect with.	**.458**	.016	.133	.189	-.059
12. I find it hard to tell if someone can be trusted.	.444	.008	.077	-.152	.044
13. I have been talked into buying something I didn't really want.	.440	-.051	.216	-.121	-.044
14. I usually find it easy to agree with others in a group.	.385	.208	.174	.250	-.098
15. Forceful people make me feel uneasy.	.373	.235	.153	-.029	.201
16. I usually give others the benefit of the doubt.	.366	.001	.005	.250	-.026
17. I don't like to rush my decisions.	.032	**.705**	-.125	.123	.050
18. I prefer to take my time to think things through.	.023	**.645**	.044	.075	.114
19. I prefer to get decisions over with quickly.	.214	**-.502**	.182	.216	.181
20. People tell me I sometimes make rash decisions.	.189	**-.486**	.371	-.088	.257
21. I prefer to read contracts for myself rather than believe what others tell me is in them.	-.154	**.485**	-.011	-.061	.241
22. I always check the small print.	-.126	**.454**	-.096	-.005	.336
23. I often seek advice from friends and family before making financial decisions.	.114	.406	.162	-.014	.003
24. I never bother double-checking terms and conditions.	.105	-.335	.316	.150	-.163

Question	Component				
	1	2	3	4	5
25. It's not important to read all of the details before making important decisions.	-.006	-.312	.195	.251	.031
26. If I like something, I have to have it straight away.	-.064	-.070	**.739**	.022	.058
27. I get a buzz from buying new things.	-.001	.089	**.706**	.057	-.056
28. I am prepared to take a risk when buying something I really want.	.013	-.013	**.674**	.036	-.053
29. I feel compelled to act immediately when I see a bargain.	.206	.066	**.549**	.185	-.018
30. I am always careful to think about things I buy.	.169	.268	**-.513**	.145	.197
31. I have made mistakes when trusting people in the past.	.262	.010	.345	-.285	.113
32. The Authorities, overall are effective at protecting us from crime.	.033	.077	.051	**.592**	-.161
33. I feel safe from becoming a victim of crime.	-.085	-.092	-.157	**.558**	.069
34. Scammers and fraudsters normally will get caught in the end.	-.001	.110	.199	**.540**	-.045
35. Only gullible people fall for scams.	-.092	-.121	.038	**.488**	.181
36. I am always careful to check out people and companies if I haven't bought from them before.	-.079	.056	-.070	.036	**.624**
37. I am always careful to check that emails and websites are real.	-.053	.039	-.195	.185	**.582**
38. I am always suspicious of people who ask me to make quick decisions.	-.128	.138	.070	-.197	**.538**
39. When something seems too good to be true, it usually is.	.003	-.160	-.273	-.112	**.492**
40. I often double-check what other people tell me.	-.066	.189	.013	-.075	**.451**
41. I avoid making decisions if someone is pressing me to choose.	-.162	.222	.068	-.116	.431
42. I tend to only buy from companies and brands that I know.	.182	.017	.042	.277	.417
43. I normally avoid making decisions when I am feeling anxious.	.201	.152	.036	.012	.364
44. You can never be sure if emails and websites are real.	.186	-.104	.127	-.213	.282
45. I am responsible for deciding what happens to me in every situation.	-.164	-.117	-.060	.181	.263
Eigenvalues	3.55	2.48	1.92	1.67	7.39
Percentage of variance	16.41	7.88	5.50	4.27	3.72

Note.
Primary factor loadings with the parent factor are shown in bold

The second factor extracted accounted for 7.88 % of the variance in participants' responses and related to the extent to which the respondent took the time to process information before making decisions. This factor loaded most heavily on questionnaire items relating to not rushing decisions and preferring to think things through and was therefore named 'Decision time'. It consisted of 4 items (Cronbach's $\alpha = .65$). Positive loadings on this factor indicated a preference for careful consideration before making decisions while negative loadings on this factor may indicate a tendency to make decisions quickly.

The third factor extracted accounted for 5.50 % of the variance in participants' responses and related to lack of restraint or risky behaviour when it comes to making purchases. This factor loaded most heavily on questionnaire items relating to not being able to resist a bargain, taking risks or an impulse to act immediately when buying something that is desired. This factor was named 'Impulsivity' and consisted of 4 items (Cronbach's $\alpha = .73$). Positive loadings on this factor indicated greater impulsivity and a disregard for risk.

The fourth factor accounted for 4.27 % of the variance in participant responses and related to the perception of justice. This factor loaded most heavily on questionnaire items relating to feeling safe from becoming a victim of a crime, whether criminals get caught and the authorities being affective in protecting people from harm. This factor was named 'Belief in justice' and consisted of 4 items (Cronbach's $\alpha = .48$), with positive loadings indicating that a person is more likely to believe that justice prevails and people get what they deserve.

The fifth and final factor accounted for 3.72 % of the variance in participant responses and related to awareness of people's motives and being cautious. This factor loaded most heavily on questionnaire items relating to verifying information, people or websites and being aware of people's motives in certain situations. This factor was therefore, named 'Vigilance' and consisted of 5 items (Cronbach's $\alpha = .65$). Positive loadings on this factor indicated increased suspicion of others' motives and readiness to cross check information given. The final version of the Susceptibility to Fraud Scale (STFS) can be found in Appendix 7.6.
Positive loadings on this factor may indicate awareness of others' motives and readiness to cross check information given.

Whilst principal components analysis considers variance and exploratory factor analysis considers covariance, both can be used for reducing the number of variables and observing the emerging patterns (Tabachnick & Fidell, 2007, p.635). Additionally, some researchers argue that there are often no differences between the two methodologies (Schonemann, 1990; Thompson, 2004) and principal components analysis has been used in scale development in the past (Gudjonsson, 1887; Sapp & Harrod, 1993). However, some researchers argue against the use of principal components analysis, suggesting that factor analysis is more suitable (Bentler & Kano, 1990; Costello & Osborne, 2005; Ford, MacCallum & Tait, 1986).
Due to this, and in order to examine whether factor structure would remain the same, exploratory factor analysis, using principal axis factoring extraction was also conducted.

Kaiser-Meyer-Olkin measure of sampling adequacy, 0.86 and Bartlett's test of sphericity (χ^2 (990) = 6382.7, p< .001) indicated that the data were suitable for factor analysis. Oblique rotation was used to determine factor composition. Initial item loadings for each of the five factors are shown in Appendix 1.7, Table 1.10.

The factor structure remained stable with both techniques, with all 26 items selected for the final version of the newly developed STFS, remaining the strongest contributors to their parent factor. One minor difference was observed with regards to item ' I never bother double-checking terms and conditions.' This question was associated with Decision Time factor using the principal components analysis but associated with Impulsivity using principal axis factoring. However, correlations for this item were not very strong to either factor.

4.3.3.2 Reliability considerations

The overall reliability of the newly developed STFS was α = .63, under the value of α =.7 recommended by DeVellis (2012) or α = .8 recommended by Field and Hole (2003). However, the overall reliability is not expected to be high in multifactorial measures. Reliability test results and means for STFS subscales are shown in Table 4.4.

Table 4.4
Reliability values and means for subscales of the Susceptibility to Fraud Scale (*N*= 536)

Factor	Number of items	Cronbach α	M	SD
Compliance	9	.87	2.82	0.81
Decision Time	4	.65	3.66	0.68
Impulsivity	4	.73	3.05	0.85
Belief in Justice	4	.48	2.76	0.67
Vigilance	5	.65	3.85	0.65

The scale yielded two scales (Compliance and Impulsivity) with reliability over .7 and two factors (Decision Time and Vigilance) just under this value. The final factor, Belief in Justice showed poor internal consistency. The lower reliability of some of the subscales may in part be explained by the fact that some subscales had fewer questions. For example, Pallant (2013) suggests that with scales with fewer than ten items, it is common to find lower values of alpha, with some as low as .5 (also Tavakol & Dennick, 2011). Sapp and Harrod (1993) accepted a range .5 to .7 as an indication of moderate reliability (Nunnally, 1967, 1978) for their brief Locus of Control scale, due to the fact that each factor had only three items.

The low reliability of the Belief in Justice Scale suggests that participants were not responding consistently to the four questions in the scale, even though this remained a consistent component of the factor analysis solution at each iteration of the analyses conducted. The scale items may therefore correlate weakly, even though they group together under a single factor. One item is measuring people's attitudes to victims of fraud. Research has found that often victims of fraud are seen as responsible for the victimisation and even victims of fraud expressed this attitude (Cross, 2013), however most of the participants disagreed with this statement.

One reason for low inter-item correlations within the subscale could be due to a lack of variability in participant responses on some items. Examination of the distribution of responses to each item however suggested this was not the case:

- 62% of participants disagreed that *Only gullible people fall for scams*
- 52% disagreed that *Scammers and fraudsters normally will get caught in the end*
- 47% disagreed that *The Authorities, overall are effective at protecting us from crime*
- 55% agreed that they *feel safe from becoming a victim of crime*

Participants' responses to all subscale items were therefore well distributed across the possible response range. For short scales with lower reliability coefficients, Pallant

(2013) recommends examining the correlations between scale items, with inter-item correlations of between .2 and .4 recommended (Briggs & Cheek, 1986). Therefore, inter-item correlations were examined for all the subscales and are reported in Table 4.5.

Table 4.5
Mean inter-item correlations for the subscales of the Susceptibility to Fraud Scale (*N*=536)

Subscales/ Questions	**Mean Subscale inter-item correlation**	**α if item deleted**
Belief in Justice		
1. I feel safe from becoming a victim of crime.	.17	.44
2. Scammers and fraudsters normally will get caught in the end.	.14	.39
3. The Authorities, overall are effective at protecting us from crime.	.22	.36
4. Only gullible people fall for scams.	.17	.45
Compliance		
1.I find it hard to say no to people without seeming rude.	.45	.85
2. I normally give in when people pressure me to make a decision.	.44	.85
3. I often find myself agreeing to things I don't really want to do.	.45	.85
4. I find it hard to say no to people I like.	.46	.84
5. People tell me I am easy to persuade.	.43	.85
6. I often worry about disappointing people.	.39	.85
7. When I find myself in a difficult situation I often make decisions I later regret.	.33	.86
8. I would prefer to be impolite rather than agree to something I don't want to do. *	.35	.86
9. I feel others often take advantage of me.	.43	.85
Vigilance		
1. I am always suspicious of people who ask me to make quick decisions.	.24	.63
2. I often double-check what other people tell me.	.24	.62
3. I am always careful to check that emails and websites are real.	.32	.56
4. I am always careful to check out people and companies if I haven't bought from them before.	.32	.56
5. When something seems too good to be true, it usually is.	.31	.62
Impulsivity		
1. I feel compelled to act immediately when I see a bargain.	.38	.68
2. I get a buzz from buying new things.	.41	.66
3. I am prepared to take a risk when buying something I really want.	.40	.67
4. If I like something, I have to have it straight away.	.41	.65
Decision time		
1. I prefer to take my time to think things through.	.28	.62
2. I prefer to get decisions over with quickly. *	.29	.61
3. People tell me I sometimes make rash decisions. *	.33	.56
4. I don't like to rush my decisions.	.39	.51

Note.
* Reverse item

This analysis indicated that overall, the mean inter-item correlation for each question with other items on the Belief in Justice scale were low when compared to mean-item correlations for other subscales which accounts for the low observed alpha value. Removal of further items from the scale however did not lead to an increase in the alpha value (Table 4.5).

The correlation between question items 2 and 3 on the Belief in Justice subscale was within recommended range (r =.36), as was the correlation between question items 1 and 4 (r =.24), while all other correlations were below .2. This may suggest stronger links exist between pairs of questions, rather than between all of the items in this subscale. Given that these questions link to popular misconceptions about scam victims and authorities found in Study 1, they may have value in their own right, which is why they were retained. The factor was therefore included in subsequent analyses.

4.3.3.3 Concurrent validity

Concurrent validity was assessed by examining the relationship between scores of the newly developed Susceptibility to Fraud Scale (STFS) with the Susceptibility to Persuasion Scale, developed by Modic and Lea (2013), which can be found in Appendix 1.5.1). The Susceptibility to Persuasion Scale measures related constructs and it was expected that there would be a positive relationship between several factors of STFS and Susceptibility to persuasion scale (Table 4.6).

A strong positive correlation (r =.60) was found between the STFS Compliance scale and Modic and Lea's (2013) Social Influence subscale, designed to indicate those that are likely to be influenced by their peers. Likewise, a strong positive correlation (r =.66) was found between the STFS Impulsivity scale and Modic and Lea's (2013) Self-control subscale, designed to reflect a lack of self-control. A moderate correlation (r =.32) was also observed between the STFS Belief in Justice scale with Modic and Lea's (2013) Trust in Authority measure, although their Need for Consistency scale was only weakly related to the STFS subscales. Taken together, the pattern of results observed supported the presence of relationships between different components of the two questionnaires, which should be theoretically related but that several STFS subscales may provide a more nuanced interpretation of need for consistency.

Table 4.6
Relationship between STFS and Modic and Lea (2013) Susceptibility to Persuasion scale, (*N* =536)

	Susceptibility to Persuasion Scale			
Susceptibility to Fraud scale	Trust in authority	Social influence	Self-control (lack of)	Need for consistency
Compliance	.10	.60*	.34*	.16*
Vigilance	-.19*	-.30*	-.20*	-.14*
Impulsivity	.17*	.31*	.66*	.17*
Decision Time	.01	-.17*	-.33*	-.25*
Belief in Justice	.32*	.02	.04	.02

Note.
* p<.001 (2-tailed). The minimum accepted *p* value used in this analysis for determining statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 20) was p=.0025.

4.3.3.4 Relationship between STFS subscales and age

The relationships between the five subscales of the STFS with age were investigated using Pearson product-moment correlations (Table 4.7). Some relationships were found between the questionnaire subscales. Compliance was negatively associated with Vigilance and Decision Time, suggesting compliant individuals tend to be less vigilant and invest less time in information processing. Compliance was also positively associated with Impulsivity, suggesting that impulsive individuals also tended to show greater compliance. Conversely, a significant positive correlation between Vigilance and Decision Time suggests that vigilant individuals tend to invest more time in processing information and making decisions.

Table 4.7
Relationship between Susceptibility to Fraud subscales and age

	Compliance	Vigilance	Impulsivity	Decision Time	Belief in Justice
Age	-.29**	.38**	-.33**	.20**	-.14*
Compliance		-.22**	.35**	-.23**	-.06
Vigilance			-.17**	.21**	-.08
Impulsivity				-.31**	.09*
Decision Time					-.06
Belief in Justice					

Note.
* Minimum accepted *p* value for statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 15 = .0033.
** p<.001 (2-tailed).

Significant positive correlations were found between age and Vigilance (*r* =.38); and age and Decision Time (*r* = .20), indicating that older individuals may be more vigilant

and invest more time in information processing. Significant negative correlations were observed between age and Compliance (r = -.38); and between age and Impulsivity (r = -.33) suggesting younger respondents tended to be more impulsive and comply with others more readily. A weak negative relationship (r = -.14) was also found between age and Belief in Justice, and a weak positive relationship (r =.09) was found between Impulsivity and the Belief in Justice, suggesting respondents that believe in justice tended to be younger and more impulsive.

4.3.3.5 Susceptibility to fraud and previous fraud victimisation

Independent-samples t-tests were conducted to compare those who have never been fraud victims and those that reported being defrauded in the past. Based on this initial analysis, only one significant difference was found after using Holm-Bonferroni adjustment for Type I error (Holm, 1979), with previous victims of fraud scoring lower than non-victims on the Belief in Justice scale, suggesting that fraud victimisation influences one's perceived view of justice (Table 4.8).

Table 4.8
Comparison of groups 'Non-victim' (N=422) and "Previous fraud victim' (N=114) and the subscales of Susceptibility to Fraud Scale using independent samples t-tests (534 df)

Subscale	Non-Victim		Previous Fraud Victim		*t*	*p*	Cohen's *d*
	Mean	*SD*	*Mean*	*SD*			
Compliance	2.80	0.82	2.88	0.73	-1.01	.32 ns	0.10
Vigilance	3.85	0.65	3.85	0.66	-0.01	.99 ns	0.00
Impulsivity	3.02	0.86	3.20	0.84	-1.49	.14 ns	0.21
Decision Time	3.68	0.68	3.58	0.70	1.37	.17 ns	0.14
Belief in Justice	2.80	0.67	2.61	0.64	2.72	.007*	0.29

Note.
* Minimum accepted p value for statistical significance reached (using Holm-Bonferroni adjustment for Type I error)

Given that prior exposure to risk will not be the same for younger and older participants, and the fact that non-victims (M = 27.75, SD = 13.90) were found to be significantly younger than previous victims of fraud (M = 32.37, SD = 15.00); t(534) = -3.10, p =.002), the comparison of STFS subscales between victims and non-victims was repeated whilst controlling for participants' ages. Independent groups analysis of covariance (ANCOVA) was used to compare the two groups, with age as a covariate (Table 4.9).

Table 4.9
Comparison of groups 'Never scammed' (*N*=422) and "Scammed once or more' (*N*=114) and the subscales of Susceptibility to Fraud Scale using one-way ANCOVA with age as a covariate (1,533 df)

Subscale	Non-Victim			Previous Fraud Victim			*F*	*p*	Partial eta-square
	Adjusted Mean	95% CI Lower	Upper	Adjusted Mean	95% CI Lower	Upper			
Compliance	2.78	2.71	2.86	2.94	2.80	3.09	3.95	.047	.007
Vigilance	3.86	3.80	3.92	3.78	3.67	3.89	1.54	.215ns	.003
Impulsivity	3.00	2.93	3.08	3.23	3.08	3.38	7.22	.007	.013
Decision Time	3.69	3.63	3.76	3.55	3.42	3.67	4.19	.041	.008
Belief in Justice	2.79	2.73	2.86	2.63	2.51	2.75	5.46	.020	.010

Note.
Bonferroni corrected *p* values shown

After adjusting for age, significant differences were found between victims and non-victims with respect to Compliance, Impulsivity, Decision Time and Belief in Justice, but not Vigilance with previous victims of fraud being more compliant, impulsive and investing less time in decision making than non-victims.

4.3.3.6 Authenticity of email correspondence; 'genuine email' vs 'phishing email'

To evaluate participants' ability to correctly identify genuine email correspondence from a phishing email attempt, two email examples from a well-known technology company were used as test stimuli. For the genuine email, 339 participants (63%) were able to recognise this as genuine correspondence and 197 participants (37%) incorrectly identified this as a fake message. For the phishing email, 132 participants (25%) incorrectly identified this as a genuine correspondence and 404 participants (75%) correctly identified this as a phishing attempt.

The only significant finding regarding the genuine email correspondence was connected to impulsivity. People who thought the genuine email was fake scored lower on impulsivity than those who correctly identified it as genuine (Table 4.10).

Table 4.10
Mean STFS subscale scores for participants identifying a Genuine email as 'real' (N = 339) or 'fake' (N =197)

Subscale	Email correctly identified as Real		Email incorrectly identified as Fake (false positive)		*t*	*p*	Cohen's d
	Mean	SD	Mean	SD			
Compliance	2.85	0.80	2.76	0.82	1.32	.189ns	0.11
Vigilance	3.80	0.63	3.91	0.68	-1.83	.068ns	-0.17
Impulsivity	3.14	0.83	2.91	0.87	2.99	.003*	0.27
Decision time	3.63	0.67	3.72	0.70	-1.60	.110ns	-0.13
Belief in justice	2.77	0.67	2.74	0.66	0.53	.594ns	0.05

Note.
* Minimum accepted *p* value for statistical significance reached (using Holm-Bonferroni adjustment for Type I error)

However, the newly developed Susceptibility to Fraud Scale (STFS) was able to discriminate between people who could correctly identify the fake email as fake and those that could not (Table 4.11).

Table 4.11
Mean STFS subscale scores for participants identifying a Fake email as 'real' (N = 132) or 'fake' (N= 404)

Subscale	Email incorrectly identified as Real (false negative)		Email correctly identified as Fake		*t*	*p*	Cohen's d
	Mean	SD	Mean	SD			
Compliance	3.00	0.77	2.76	0.81	2.98	.003*	0.30
Vigilance	3.65	0.66	3.90	0.64	-3.92	<.001*	-0.38
Impulsivity	3.39	0.80	2.94	0.84	5.34	<.001*	0.55
Decision time	3.52	0.64	3.71	0.69	-2.81	.005*	-0.29
Belief in justice	2.86	0.65	2.72	0.67	2.00	.046*	0.21

Note.
* Minimum accepted *p* value for statistical significance reached (using Holm-Bonferroni adjustment for Type I error)

The findings indicate that vigilant individuals and those that invest more time in making decisions were better at recognising a phishing attempt, whilst those with higher scores in compliance, impulsivity and belief in justice were less able to do so.

Individuals that were more compliant and more impulsive were more likely to identify fake email as genuine. These results suggest the newly developed Susceptibility to Fraud Scale has good discriminant validity when it comes to phishing correspondence

4.3.3.7 Confidence ratings in classifying email correspondence

As well as being asked to decide if an email example they were presented with is a genuine email or a phishing email, participants were asked to rate how confident they were about their decision on a scale of 1 (not at all confident) to 10 (extremely confident). Using a 2x2 mixed ANOVA, differences in confidence between those that have never been defrauded and those that reported they were defrauded in the past were tested.

The main effect for type of correspondence (fake or genuine) was significant ($F_{(1, 534)} = 7.91, p = .005, \eta^2_p = .015$). However, the main effect for scam group was not significant ($F_{(1, 534)} = 2.93, p = .087, \eta^2_p = .005$) and there was no interaction between scam group and type of email ($F_{(1, 534)} = .130, p = .719, \eta^2_p = .000$).

These results suggest there are no differences between those that have never been defrauded and those that have, when it comes to how confident people are that they predicted the authenticity of email correspondence correctly. However, participants were less confident in their answer when rating the genuine email than when they were rating the fake email (Figure 4.2).

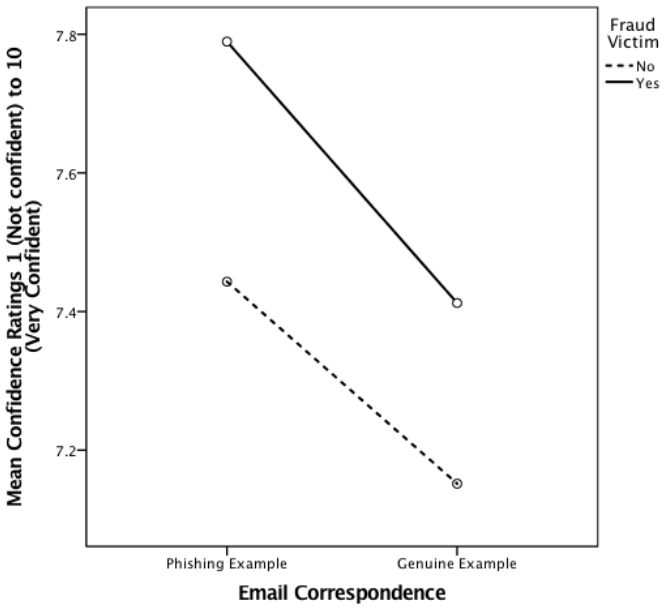


Figure 4.2 Confidence ratings reported by fraud victims (*N*=422) and non-victims (*N*=144) when evaluating genuine and phishing email correspondence

There were no differences in confidence between participants who correctly identified the genuine email as real and participants who incorrectly identified it as fake. However, participants that incorrectly identified the phishing email as real were less confident in their answer than those that made a correct identification (Table 4.12).

Table 4.12
Participants' mean confidence ratings when rating authenticity of email correspondence (534 df)

Confidence Ratings	Email correctly identified			Email incorrectly identified (false positive)			*t*	*p*	Cohen's d
	N	Mean	SD	N	Mean	SD			
Genuine email	339	7.09	1.75	197	7.42	2.23	-1.90	.058	-0.16
Fake email	404	7.91	2.00	132	6.32	1.96	-7.99	<.001	-.0.80

Pearson Product-Moment Correlations of confidence ratings to examine relationships between subscales of the STFS and victim group (non-victim and previous fraud victim). Results are presented in Table 4.13.

Table 4.13
Pearson Product-Moment Correlations showing the relationships between the STFS subscales and confidence when rating authenticity of email correspondence (rated from 1, Not at all confident to 10, Extremely confident) for previous fraud victims (*N*=422) and non-victims (*N*=114).

Subscale	Non-Victim		Previous Fraud Victim	
	Confidence ratings for genuine email	Confidence ratings for fake email	Confidence ratings for genuine email	Confidence ratings for fake email
Compliance	-.02	-.20*	-.04	-.19
Vigilance	.18*	.28*	.14	.26
Impulsivity	.04	-.16*	-.02	-.27
Decision Time	-.01	.10	.02	.28
Belief in Justice	.08	-.05	.01	-.08

Notes.
The minimum accepted *p* value used in this analysis for determining statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 20) was p=.0025.
* p< .001 (2-tailed).

A significant positive correlation was found between Vigilance (r =.18) with confidence ratings for the genuine email, and Vigilance (r =.28) with confidence ratings for the fake email. This suggests that more vigilant individuals had higher confidence in their answers when classifying email correspondence, both genuine and fake.
Significant negative correlations were found between Compliance (r = -.20) with confidence ratings for the fake email; and Impulsivity (r = -.16) with confidence ratings

for the fake email, suggesting that more compliant and more impulsive individuals had lower confidence in their answer when classifying fake email correspondence.

4.3.3.8 Scam scenarios

Participants were also given 7 (out of the 9) scenarios used by Modic and Lea (2012) as measures of susceptibility to scams, in order to see if there was a relationship between the subscales of the newly developed STFS subscales and scam scenarios. The scenarios can be found in Appendix 1.5.2. The store credit card scenario was not a scam but was included as a control to evaluate whether participants could tell which situations scammers might exploit. A detailed breakdown for each scenario is provided in Table 4.14.

Table 4.14
Scam scenarios mean ratings and percentage of participants that 'received', 'responded to' and 'lost money' to such an offer (N = 536)

Scam Scenario	Mean Rating (out of 5) and 95% CIs		Number of Respondents		
	Likelihood of event being a scam	Likelihood of general public responding favourably to it	Previously received such an offer (%)	Previously responded to such an offer (%)	Previously lost funds to such an offer (%)
Bank phishing email	3.81 [3.70, 3.91]	3.60 [3.51, 3.69]	36.9	5.8	1.9
Nigerian scam	4.73 [4.66, 4.80]	2.16 [2.07, 2.26]	32.6	0.7	0.4
Auction scam	4.35 [4.28, 4.42]	3.27 [3.17, 3.36]	7.1	3.0	1.3
Investment scam	3.85 [3.77, 3.93]	3.10 [3.01, 3.19]	4.1	0.4	0.2
Classified ads scam	3.36 [3.26, 3.46]	3.52 [3.45, 3.60]	4.1	1.7	0.4
Pyramid scheme	3.85 [3.77, 3.94]	3.14 [3.05, 3.23]	9.9	0.9	0.4
Store credit card/ (Non-scam control)	1.85 [1.77, 1.92]	3.95 [3.87, 4.03]	49.3	15.3	1.3

Modic and Lea (2012) reported that 30% of participants had experienced at least one the scenarios used, 13% had responded to at least one scenario, but only around 1% of their participants had lost money to such scenarios in the past three years. The present study found that 55% of participants reported finding themselves in at least one of the situations used, 9% reported responding and 3% reported losing money to at least one scam scenario.

Using repeated measures ANOVA, differences in likelihood of each scam scenario being a scam were tested. Mauchly's test indicated that the assumption of sphericity had been violated ($\chi^2(2)=110.99, p < .001$, W=.81), therefore the degrees of freedom were corrected using Greenhouse-Geisser estimates.

A significant difference was observed in the likelihood ratings of each scenario being a scam ($F_{(5.61, 2999.62)} = 606.87, p < .001, \eta^2_p = .53$), with the Nigerian scam and auction scam scenarios being rated as the most likely to be a scam. The store credit card was rated as the least likely to be a scam and was therefore excluded.

Repeated measures ANOVA was also used to test for differences in the likelihood that the general public would respond favourably to the scam scenarios. Mauchly's test indicated that the assumption of sphericity had been violated ($\chi^2(2)=142.29, p < .001$, W=.77), therefore the degrees of freedom were corrected using Greenhouse-Geisser estimates.

A significant difference was observed for the likelihood of the general public responding favourably to the scam scenarios ($F_{(5.49, 2935.23)} = 211.90, p < .001, \eta^2_p = .28$). The Nigerian scam scenario was rated as being the least likely to result in a favourable response, while the in-store credit card was rated as the most likely to result in a favourable response by the general public, followed by a bank phishing email.

Cochran's Q tests were used to examine which fraudulent scenarios were the most commonly encountered or recognised by participants and which were the most commonly responded to. The store credit card scenario was excluded from these analyses, as it was not a scam. The analyses showed there was a statistically significant difference in frequencies between scenarios when it came to encountering different scam offers ($Q(5, n=536) = 499.06, p < .001$). Bank phishing emails and Nigerian scams were the most commonly encountered scams by participants, while investment and classified adverts (fake cheque) were the least common.

There was also a statistically significant difference in frequencies between scenarios when it came to responding to scams, ($Q(5, n=536) = 62.18, p < .001$). Participants reported having responded most frequently to a bank phishing email and auction scams and least frequently to an investment scam.

4.3.3.9 Relationship between the STFS and scam scenarios

The relationships between the subscales of the STFS and different scam scenarios are shown in Table 4.15. The STFS Impulsivity subscale scores correlated negatively with all 6 true scam scenarios, whilst the STFS Compliance scale scores were negatively correlated with all but one scenario (Nigerian scam). This suggests that those who scored higher for compliance and impulsivity seemed to be less able to recognise that the presented scenarios could potentially be fraudulent offers. In contrast, positive correlations were found for age and for the STFS Vigilance subscale with the 6 true scam scenarios, suggesting that older and more vigilant individuals were more likely to recognise that the scenarios could potentially be used to defraud. The STFS Decision Time scale correlated positively but only weakly with the scam likelihood ratings for 3 of the 6 true scam scenarios, and no significant correlations were found between Belief in Justice and participants evaluations of the different scenarios.

Table 4.15
Pearson Product-Moment Correlations showing the relationships between the STFS subscales, age and subjective likelihood ratings that the scenario may be a scam (rated from 0, Extremely Unlikely to 5, Extremely Likely) (*N*=536).

Scam Scenario	Age	Compliance	Vigilance	Impulsivity	Decision Time	Belief in Justice
Bank phishing	.40**	-.20**	.33**	-.19**	.20**	-.13
Nigerian scam	.16**	-.05	.14*	-.14*	.06	-.06
Auction scam	.27**	-.15**	.28**	-.18**	.15**	-.13
Investment scam	.42**	-.13	.25**	-.22**	.13	-.11
Classified ads scam	.54**	-.26**	.34**	-.29**	.17**	-.11
Pyramid scheme	.41**	-.18**	.25**	-.22**	.10	-.07
Store credit card/ (Non-scam control)	.12	-.10	.07	-.09	.08	-.02

Notes.
* p< .0012 (2 -tailed) Minimum accepted *p* value for statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 42).
** p< .001 (2-tailed).

The number (out of 6) of the true scam offers that participants reported having previously received, responded to, or lost money over were totalled for each participant. In order to examine participants past experience and behavioural responses to the 6 different true fraudulent offers in relation to the STFS subscales, point-biserial correlations were calculated (Table 4.16).

Table 4.16
Point-Biserial Correlations between STFS subscales and age with previous experience of receiving or responding to one or more scams (0=No; 1=Yes) (*N*=536).

	Previously received such an offer	Previously responded to such an offer	Previously lost money to such an offer
Age	.33**	-.11	-.08
Compliance	-.08	.08	.08
Vigilance	.23**	-.10	-.11
Impulsivity	-.04	.16**	.15**
Decision Time	-.002	-.13*	-.10
Belief in Justice	-.07	.03	-.04

Notes.
* p< .003 (2 -tailed) Minimum accepted *p* value for statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 18).
** p< .001 (2-tailed).

A significant positive correlation was observed between STFS Vigilance scores and those reporting that they had found themselves in one or more situation similar to scenarios they evaluated in the past 3 years. This may indicate that vigilant individuals might be better at recognising fraudulent situations when they encounter them. A similar pattern was also observed for age. The STFS Impulsivity and Decision Time subscales both correlated significantly with responding to fraudulent offers in the past, suggesting that impulsive individuals were more likely to respond to and lose money to potential fraudulent offers, whilst individuals that take more time to make decisions were less likely to respond to fraudulent offers.

4.4 Scale Development Study Discussion: Study 2

The literature review in Chapter 2 identified the need for more individual approach to studying susceptibility to fraud. Individual characteristics have been found to predict the likelihood of responding to fraudulent offers as well as attitudes towards privacy and security (Egelman & Peer, 2015; Modic & Lea, 2012, 2013). However, there are, at present, no widely available measures with regards to fraud susceptibility. Modic and Lea's (2013) Susceptibility to Persuasion scale is the only available scale measuring concepts related to fraud vulnerability (developed further by Modic & Anderson, 2014a) and the present study builds on this research.

The development of the 26-item Susceptibility to Fraud Scale (STFS) took into account extensive research on fraud and fraud victimisation as well as available theories of constructs that may be related to susceptibility to fraud. The scale yielded five factors that may contribute to individual's vulnerability to fraud; Compliance, Vigilance, Impulsivity, Decision Time and Belief in Justice and was able to discriminate between people who could correctly identify phishing email correspondence as fake and those that could not. Vigilant individuals and those that invest more time in making decisions were better at recognising a phishing attempt while compliant and impulsive individuals as well as individuals who believe in justice more readily were less able to do so.

STFS was also able to discriminate between previous fraud victims and non-victims. Previous fraud victims were found to be more compliant, impulsive and seem to invest less time in decision making than non-victims. Although previous fraud victims did not differ from non-victims in the amount of vigilance they possess, this may be down to the fact that most fraud victims become more vigilant as a result of fraud victimisation. Additionally, although participants that have previously been defrauded did not feel any more confident judging email correspondence than non-victims, more vigilant individuals had higher confidence in their answers for both, genuine and fake email correspondence.

When participants were given real life scenarios, that could potentially be fraudulent, to consider, vigilant individuals were more able to recognise that the presented scenarios could potentially be fraudulent situations. In contrast, compliant and impulsive individuals were less able to recognise the scenarios could be fraudulent situations. They also felt less confident in their answer when classifying phishing email correspondence. This suggests that vigilance may be a protective factor when it comes to fraud vulnerability.

4.4.1 Factors of the Susceptibility to Fraud Scale

Compliance proved to be the most internally consistent factor. Individuals with high scores on this factor would be more likely to comply with others due to activation of social norms or other factors, such as time pressures, despite awareness of the vulnerability. Questionnaire items for this factor relate to factors found to increase vulnerability to fraudulent offers, such as liking and similarity and evoking social norms (Lea et al., 2009). Compliance predicted individuals that incorrectly identified phishing

correspondence as genuine as well as those that reported being defrauded in the past. Therefore, this subscale may be a good measure of general compliance with fraudulent offers.

Impulsivity was the second most reliable factor. Individuals with high scores on this factor may exhibit lack of restraint and disregard to risk with regards to making purchases. Impulsivity predicted those that incorrectly identified phishing correspondence as genuine. This suggests that Impulsivity subscale may be a good measure of lack of restraint when it comes to purchases, which could be exploited by scammers, but could also be applied to other types of fraud. Impulsivity also predicted previous fraud victimisation.

Impulsivity was also positively related to lack of self-control, a subscale of Modic and Lea's (2013) Susceptibility to Persuasion scale, which was found to predict responding to fraudulent offers. In an earlier study, Modic and Lea (2012) found that premeditation, a facet of an impulsivity measure, also predicted responding to fraudulent offers. Current findings confirm this. Using Modic and Lea (2013) scam scenarios, the present study found that more impulsive individuals were more likely to respond and lose money to fraudulent situations similar to the scam scenarios they were assessing.

Vigilance was related to awareness of others' motives and readiness to check the information. Questionnaire items measuring vigilance are related to research on trust and vigilance (Greenspan, 2009; Markóczy, 2003) as well as research identifying scepticism as a moderator of scamming vulnerability (Langenderfer & Shimp, 2001). It also refers to the motivation to process information (Lea et al., 2009).
Research on trust and vigilance found that vigilance was found to be implicated in predicting the behaviour of others (Markóczy, 2003), with trusting but vigilant individuals better at predicting how others would behave. Although this factor had lower reliability than the previous two factors, Vigilance predicted correct identification of phishing correspondence and previous fraud victimisation.

This subscale may be a good indication of individual's willingness to be cautious and check the information provided, which would help protect one from fraudulent offers. Vigilant participants reported they found themselves to be in receipt of a greater number

of scam offers of the type described in the scenarios used in the present study (Modic & Lea, 2013). This may be down to their heightened awareness of fraud in everyday situations. Grabosky and Duffield (2001) suggested that fraud victimisation is easier when one's vigilance is relaxed and that the key lies in the effective education and fraud prevention systems that would swiftly detect fraud, where committed. It could therefore be argued that individuals with higher levels of vigilance and awareness with regards to fraud would be more protected from fraud victimisation.

Decision Time indicates a preference to take more time to carefully consider information when making decisions. It was also found to have lower reliability than Compliance and Impulsivity, however, questionnaire items for this factor relate to the data from the first study in this programme of research (Chapter 3), interviews with victims of fraud, where majority of the participants reported they regret rushing their decisions. Questionnaire items for this factor also relate to the literature on gullible action (Greenspan, 2009). Decision Time successfully predicted correct identification of phishing correspondence and previous victimisation; therefore, this subscale may be a good measure of vulnerability to fraud. Additionally, those that reported taking greater time when making decisions were less likely to have previously responded to fraudulent offers. This supports the assertion by Greenspan (2009) that delaying decisions, in certain situations, offers protection from gullible action.

Positive relationships were found between Vigilance and Decision Time. Participants who exhibited greater vigilance were also found to invest more time in making decisions. Since both characteristics were found to be good predictors of correct scam identification, when it came to recognising the phishing correspondence example used in the present study, it may be assumed that Vigilance and Decision Time are protective factors that help lower the risk of fraud victimisation.

The Belief in Justice subscale was intended to capture people's attitudes towards fraud victims as well as fraud agencies and processes that can be applied once fraud victimisation takes place. The items on this factor relate to data from the interview study in Chapter 3, on people's reactions to justice, following the victimisation (also Lea et al., 2009) and discourse regarding fraud victims (Cross, 2013, 2015). For example, many participants in the first study reported that they believed that if they

were defrauded, the case would be investigated and the perpetrator caught. Lea et al. (2009) suggested this notion relates to the illusion of control.

Individuals that expressed a greater belief in justice tended to be younger and were less likely to have been a previous victim of fraud. The finding that previous victimisation appears to lower one's belief in justice could in part be down to the experience of participants when reporting fraud to relevant agencies and not getting the desired response. Previous research has found that fraud victims have a strong desire for justice following fraud victimisation but often even the basic advice or help is unavailable (Button, et al., 2013; Button et al., 2015). However, since this factor had much lower reliability than recommended, these findings should be taken with caution as this factor warrants further testing in order to ascertain its reliability and validity.

The newly developed Susceptibility to Fraud Scale is one of the first specifically developed scales to measure vulnerability to fraud. However, reliability of the whole scale and some of the factors was lower than the alpha value recommended by DeVellis (2012). Although the scale demonstrated content, concurrent and predictive validity, the reliability of some of the scales lets it down, therefore the scale would benefit from further testing.

4.4.2 Age and fraud vulnerability

Age was found to be an influential factor in contributing to fraud vulnerability. Younger participants self-reported that they exhibited more compliant and impulsive behaviour, which in turn were connected to lower detection of potential fraudulent situations, as measured by participants' responses to the example scam scenarios used in the present study. In addition, compliance and impulsivity were connected to reduced time invested in making decisions and processing information with participants that reported being victims of at least one or more scams being more likely to exhibit these characteristics. Older participants self-reported being more vigilant and taking more time when making decisions. They were also more likely to report finding themselves in receipt of fraudulent offers in the past 3 years. As this was also true of vigilant individuals, it could mean that with age, people become more vigilant and better at recognising fraudulent offers when they encounter them. Although older participants in the present study seemed to exhibit characteristics that may help protect against experiencing fraud victimisation, it cannot be argued that age reduces vulnerability.

Elderly people are known to be aggressively preyed upon by scammers and so remain one of the most vulnerable groups when it comes to fraud through an increased exposure to risk (Harries et al., 2013; Langenderfer & Shimp, 2001). In addition, only 4% of the current sample was aged 60 years or over, when some authors have argued that cognitive decline may lead to an assumed increased in vulnerability (Langenderfer & Shimp, 2001; Lea et al., 2009; Schiebe, 2015).

4.5 Future considerations

The present study found that the newly developed 'Susceptibility to Fraud' measure was good at predicting attributes that contribute to responding to phishing correspondence. There are different kinds of phishing correspondence, some of which rely on quick decision making, usually purporting to refer to customers' compromised account that needs attention, and this is the kind we presented to participants in the present study. Testing the scale on different kinds of phishing correspondence, such as Nigerian scam correspondence, where more deliberation is required on the part of the potential victim, or other online scams (i.e. lottery scams, sweepstakes, miracle cures etc.) would be beneficial. For example, the phishing example of email correspondence presented to participants in this study contained a warning about a compromised account, which is likely to evoke panic or fear. As different types of scams rely on different motivational and cognitive factors, the scale may yield different results with scams that evoke positive emotions (e.g. lottery win or a prize) or rely on different scam cues (e.g. authority or scarcity). It would therefore, be valuable to examine if the newly developed STFS could be used as a valid general measure of vulnerability to fraud across different types of scams and what factors explain vulnerability to different types of scams best. This would also allow for the scale to be used in fraud prevention. For example, if we knew that compliance and impulsivity best predict certain types of scams and lack of vigilance other types of scams, individuals could be educated about scams that they may be more vulnerable to, according to their scores on STFS, in order to avoid future victimisation.

Although STFS was able to discriminate between people who could correctly identify phishing email correspondence as fake and those that could not, it must be noted that measuring fraud compliance by asking participants to decide if an email is real or fake

raises certain considerations. Deciding whether email is a phishing example or a real email in an online survey does not accurately represent a real-life situation. If an individual received an email, such as a warning about a potential closure or compromise of their bank account, they would most likely be experiencing strong emotions (e.g. fear or panic), which are likely to have an impact on their decisions about what to do about it. Since this is lacking in a survey, where participants are being asked to evaluate emails rationally and are not active recipients of such emails, their decisions are less likely to be governed by visceral influence or strong emotions. However, given the fact that the STFS still predicted those who incorrectly identified phishing correspondence as genuine, it is likely that it may also be a good predictor of vulnerability to phishing correspondence in real-life contexts and in the presence of additional vulnerability factors.

The present study used the same sample to develop the STFS and test its reliability and validity. Whilst this is not ideal, Study 3 (Chapter 5) was seen as an opportunity to replicate the reliability tests, as well as test the validity of the newly developed STFS on an independent sample. The results are reported in section 5.3.1 in Chapter 5.

4.6 Conclusion

In the present study, a measure of susceptibility to fraud was developed and tested. The newly developed Susceptibility to Fraud Scale was able to discriminate between previous fraud victims and non-victims as well as participants who could correctly identify phishing email correspondence and those who could not. Additionally, STFS was also able to discriminate between participants that were able to recognise that certain real-life situations (e.g. online auctions or classified adverts) could potentially be scams. Compliance and Impulsivity, as well as Belief in Justice, were associated with increased fraud vulnerability, whilst Vigilance and Decision Time seem to moderate it. The results, therefore, suggest that Susceptibility to Fraud Scale may be used as an indicator of individual vulnerability to phishing correspondence, and could potentially also apply to other types of fraud.

The research in the present study provides an important contribution to understanding factors that underlie vulnerability to fraudulent offers, especially with regards to

protective factors, that may moderate susceptibility to fraud, such as increased vigilance and a preference to delay decisions and consider the available information. In addition, this research confirms the findings of existing research (Langerderfer & Shimp, 2001; Lea et al., 2009; Modic & Lea, 2012, 2013) on lack of self-control and impulsivity as factors that increase vulnerability to scams. These findings may also provide the basis for more individual and victim orientated approach to fraud prevention.

Chapter 5

The Barnum effect as a measure of susceptibility to fraud

5.1 Introduction

The aim of the study described in this chapter is to build on the results obtained in the previous, scale development study, Study 2. Having developed the Susceptibility to Fraud Scale (STFS) and assessed its reliability and validity against Modic and Lea (2013) Susceptibility to Persuasion scale, the STFS was tested on the examples of email correspondence, in order to examine if it could predict correct identification of a phishing correspondence. The study found that vigilant individuals, as well as individuals that prefer taking the time to make their decisions were better at recognising a phishing attempt than individuals that were more impulsive and compliant.

The next step would be to test the newly developed STFS scale in a real-life scam situation. However, there are moral and ethical considerations in doing so (Jagatic et al., 2007). Therefore, a proxy scam situation that mimics what people may experience in a real-life scam situation was used for Study 3.

5.1.1 Gullibility in relation to fraud

Gullibility is frequently associated with being too trusting, however, some studies have argued otherwise (Markóczy, 2003; Yamagishi, Kokuchi & Kosugi, 1999; Yamagishi & Kakiuchi, 2000). Rotter (1980) argued that trusting someone in the absence of warning signs is not the same as trusting someone in the presence of warning signs or evidence that the person is not trustworthy, and that only the latter is connected to gullibility. Markóczy (2003) found that trusting individuals that are also vigilant were better at predicting behaviour of others than naïve trusters. Langenderfer and Shimp (2001) argued that gullibility may enhance scam vulnerability under certain conditions. For example, Greenspan (2008) suggests that induced foolish action happens in the presence of manipulation by person(s), usually on the basis of false information against one's best interests, manifesting itself as "gullibility". Gullibility and foolish action may, therefore, in some situations, be connected to fraud vulnerability, especially where there is a direct contact with the scammer and his or her actions need to be evaluated.

5.1.2 The Barnum effect as a measure of gullibility

The Forer effect, also known as the Barnum effect, is a personal validation fallacy, referring to the acceptance of vague and widely applicable feedback as highly accurate of oneself, when presented as bona-fide personality feedback. In his study, Forer

(1949) gave participants a psychometric measure, after which he supplied them with personality feedback. Participants were told they were receiving personality feedback based on the scores of the measures they completed (i.e. their personalised feedback), however the feedback they received was the same for all participants and was derived from daily horoscopes. The feedback was purposely vague or neutral and could apply to anyone. Participants were then asked to rate the feedback for how accurate it was as a description of their personality. The study found that participants rated this highly generalised feedback as being a 'good' or 'perfect' fit to their own personality. Moreover, when participants are given their actual true personality feedback, as well as the Barnum feedback, due to its broad applicability, the Barnum feedback was seen as more accurate (O'Dell, 1972).

Several studies researching the Barnum effect have made a connection between the acceptance of bogus personality feedback and gullibility (Dana & Graham, 1976; Forer, 1949; MacDonald & Standing, 2002; Piper-Terry & Downey, 1998). However, Layne (1979) argues that accepting vague feedback as a description of one's personality does not equate to gullibility, as such feedback is purposely designed to apply to the majority of people, and as such, the acceptance of the feedback may be rational and not gullible. Personality test feedback is seen as more credible, when coming from a credible source (e.g. a psychologist), therefore it would be irrational not to accept it as accurate feedback. Personality feedback also may be regarded as more accurate when it is presented as overall feedback instead of individual statements (Layne, 1978). This may be problematic as it could lead to an inaccurate measurement of the effect.

5.1.2.1 The Barnum effect manipulations

Some studies have found that when the same, vague personality feedback is given to participants but they are asked to rate how accurate it is of people in general, the accuracy ratings for people in general tend to be lower (Snyder & Larson, 1972). For example, in the study by Johnson, Cain, Falke, Hayman and Perillo (1985), one group of participants was asked to rate the personality feedback presented to them for how accurate it is of them, and the other group was asked to how accurate it may be of their acquaintance. They did not complete any psychometric measures prior to assessing the personality feedback, which is usually the case with the Barnum effect studies. The study found that participants rated the statements as more accurate of them, despite the fact that they were not made to believe that the feedback was based on personal

information. Johnson et al. (1985) suggested that the reason for this may be down to the fact that individuals have a greater availability of knowledge about 'the self' as opposed to other people.

Other manipulations included adding positive and negative statements to the bogus personality feedback, in order to see if this influences the perceived accuracy ratings. Layne (1978) replicated Forer's (1949) original experiment but gave each participant favourable (positive) or unfavourable (negative) personality feedback and asked them to rate it for accuracy. The positive and negative statements were specific (i.e. not highly applicable), rather than neutral or vague. The study found that participants accepted favourable or positive items more readily than negative. Dana and Fouke (1979) similarly found that positive statements were rated as more accurate as were neutral statements, and suggested that this may be down to the fact that neutral and mildly positive statements may have a higher base validity (i.e. have a higher occurrence in general population) than negative items in the general population.

Several other research studies have also used positive and negative feedback, finding that people tend to rate positive items higher and negative items lower, when asked to evaluate the feedback for how accurate it is of them (Dana & Fouke, 1979; Davies, 1997; Furnham & Varian, 1988; Layne, 1978; MacDonald & Standing, 2002). When asked to rate the same feedback for 'people in general', the pattern is reversed.

In the studies by Furnham and Varian (1988), participants completed psychometric measures, after which they were given 9 positive and 9 negative personality statements to rate for accuracy on a 9-point scale. The study found that participants rated positive items as more accurate than negative. Furnham and Varian (1988) then replicated the study and used slightly different types of personality feedback, in order to overcome the confounding of the base rate validity of statements. The personality statements given to participants included; general and positive, which have a high base rate occurrence in the general population (e.g. 'Security is one of your major goals in life'), general and negative (e.g. 'You have a great deal of unused capacity which you have not turned to your advantage.'). They also included specific statements; specific positive (e.g. ' You are often described by others as the most popular person they know.') and specific negative (e.g. ' You can be very patronizing to those you see inferior to yourself.'). They found that general statements were rated as more accurate than specific, with

positive general statements rated as more accurate than negative general statements, which suggested that the acceptance of personality feedback is due to generality rather than favourability of the items.

The Barnum effect is also influenced by the perceived status of the person administering the feedback and is also known as prestige effect (Halperin, Snyder, Shenkel & Houston, 1976; Rosen, 1975; Snyder & Newburg, 1981). In the study by Rosen (1975), participants were given psychometric measures to complete, after which they were asked to provide their own and their parents' date of birth. Participants were then given the same personality feedback; however, one group was told the feedback was provided by an astrologer on the basis of the dates of birth provided while the other group was told the feedback was provided by a psychologist, based on the psychometric measures they completed. The study found that the same personality feedback was rated higher when it was provided by a psychologist than when it was provided by an astrologer.

Snyder and Newburg (1981) manipulated the prestige of the test administrator in a group setting. The group of participants were taken to an office of 'Dr. Smith' where they were greeted with a test administrator who was dressed in a professional manner. Participants took part in a discussion led by Dr. Smith, in which they introduced themselves to one another and were encouraged to share details about themselves. Participants were then asked to describe another member of the group based on the discussion they engaged in. They were also told they would receive personality feedback by Dr. Smith, based on the discussion. Finally, participants were also asked to rate how qualified they thought Dr. Smith was to provide the personality feedback and how qualified another group member is to provide personality feedback based on the discussion. Participants were then provided with bogus personality feedback, with some participants receiving positive statements and some receiving negative statements. Half of participants were told Dr. Smith provided their personality feedback and half were told another group member provided the feedback. The study found that personality feedback which was provided by Dr. Smith was rated as being more accurate than feedback provided by another group member, even when negative feedback was given (also Halperin et al., 1976). Additionally, Snyder and Shenkel (1976) tested if personality feedback would be rated differently when provided in oral rather than written form, but found no differences.

5.1.3 The Barnum effect as a proxy scam measure

Vague feedback often appears to the individual receiving it, as highly accurate feedback of his or her own personality. People do not recognise the fact that this is due to the high base rate of such feedback (i.e. high occurrence in the general population), therefore it could be equally accurate of others as it is of them. This difference in the degree to which vague and highly applicable personality feedback is true of oneself versus true of others may indicate a cognitive bias, which can be exploited for fraudulent gains. For example, this type of feedback is often part of clairvoyant or psychic scams or other cold readings, such as astrology predictions or palm readings. In fact, in the original study by Forer (1949), the statements were compiled from daily horoscopes. The inability to recognise the broad applicability of such feedback may indicate an individual's vulnerability to this type of fraud. As such, the Barnum type feedback may provide a suitable proxy scam measure for frauds that utilise this type of feedback.

The Barnum effect might also help to explain participants' responses in other potential fraudulent situations. Stajano and Wilson (2011) found that online auction scams are perpetrated by inflating the seller's customer feedback with fake testimonials, which are seen as trustworthy sources. Therefore, feedback that appears to be coming from trustworthy sources, such as a psychologist in the case of the Barnum effect studies, may be more likely to be accepted as true without consideration for its authenticity.

Many scams rely on authority cues, due to the fact that people tend to trust and obey those in authority (Lea et al., 2009; Modic & Lea, 2013; Whitty & Buchanan, 2012a, 2012b; Whitty, 2013; Workman, 2008). Therefore, fraudulent offers frequently purport to be from authority figures or someone who can facilitate the offer (Lea et al., 2009). Similarly, in the Barnum effect studies, personality feedback is based on previously scored psychometric measures and tends to be delivered by a psychologist (i.e. a person that is qualified to administer psychometric tests), therefore the accuracy assigned to the received feedback may be down to the perceived authority of the person preparing it. For example, some studies looking into the Barnum effect found that 'prestige' or status of the person that is administering and delivering personality feedback influences accuracy scores (Halperin et al., 1976; Rosen, 1975; Snyder & Newburg, 1981).

In most scam situations, there is usually some information that is processed by the potential victim, whether that is a website or email content or some other information provided by the scammer in face-to-face situations. The decision of whether to trust such information depends on different factors, many of which are manipulated by scammers, such as adding cues of authenticity or purporting to be from authority sources or even creating false endorsements to influence the victim and detract from careful information processing. Therefore, the Barnum effect paradigm may be a good way of examining acceptance of information that is not authentic when it comes from what appears to be a qualified source, especially when specific positive and specific negative feedback is used.

5.1.4 The Barnum effect and personality attributes

The Barnum effect has been linked to certain personality characteristics. Cuperman, Robinson and Ickes (2014) conducted an online survey, in which participants completed various psychometric measures one of which was the Sense of Self Scale (SOSS), after which participants were told they were to receive personality feedback based on the measures administered, which they were asked to rate for accuracy, statement by statement and overall. Participants were then given the vague statements used in the study by Forer (1949). The study found a positive relationship between the acceptance of neutral or generic Barnum effect statements and several personality predictors; self-reported self-monitoring, inner directedness, emotional contagion and a weak sense-of-self. Additionally, they found a negative relationship between the acceptance of generic personality statements and self-esteem, self-concept clarity and social desirability. Furthermore, sense of self was also identified as a predictor of the Barnum effect acceptance scores, and Cuperman et al. (2014) concluded that the Barnum effect paradigm is a good way to explore malleability of self-image in individuals with a weak sense-of-self.

The Barnum effect has also been linked to an individual's need for social approval (Mosher 1965; Orpen & Jamotte, 1975). In their study, Orpen and Jamote (1975) gave their participants a scale measuring the need for group approval, after which participants received identical personality feedback. The study found a positive relationship between social approval and acceptance of bogus personality feedback.

More recently, research by Mason and Budge (2011) found a relationship between the Barnum effect and referential thinking or a tendency to experience events as referring to one's self. In their study, participants completed different measures and were given different personality feedback to evaluate, some consisting of feedback based on one of the scales used, some horoscope derived items and positive and negative Barnum type statements developed by the authors. The study found no differences in the extent of agreement between the different types of feedback.

Acceptance of false personality feedback has also been linked to having an external locus of control (Cupperman et al., 2014; Snyder & Larson, 1972). Rotter (1966) describes locus of control as: "the degree to which the individual perceives that the reward follows from, or is contingent upon, his own behaviour or attributes versus the degree to which he feels the reward is controlled by forces outside of himself and may occur independently of his own actions" (Rotter, 1966, p 8).

External locus of control refers to the attribution of events to luck or chance or something that is beyond one's control. This also includes attributing events to the behaviour of powerful others. Internal locus of control, refers to attribution of life as being contingent upon one's own behaviour, effort or characteristics.

Contrary to previous research, studies looking into personality factors in relation to the Barnum effect by Furnham (1989), found that those with an internal locus of control accept positive and reject negative feedback more readily than those with the external locus of control. Furnham (1989) also found a positive relationship between factors associated with extraversion and positive personality feedback and factors associated with neuroticism with negative personality feedback.

5.1.5 Research aims and rationale

The present study aimed to explore whether the Barnum effect may be used as a successful proxy scam measure in order to test the utility of the newly developed Susceptibility to Fraud Scale (STFS). More specifically, can STFS predict the acceptance of positive, negative and neutral Barnum type personality feedback?

As some studies found that personality feedback is accepted more readily when the status of the experimenter appears to be higher, administering the Barnum effect

experiments online may mean that potential confounding effects would be avoided as there is no authority figure present to reinforce the feedback. However, not many Barnum effect studies have been administered online. Although their study did not use the Barnum effect, Fletcher, Taylor and Glansfield (1996) explored the acceptance of personality feedback generated by different sources. Some participants were told an expert interpreted their personality feedback and others were told it was computer generated. They found no differences in ratings for feedback that was computer generated as opposed to interpreted by an expert. More recent studies have been conducted using online survey methods (e.g. Cuperman et al., 2014), which seems to be a convenient method, as the data on both, psychometric measures and the feedback ratings can be collected at the same time, minimising attrition.

Personality feedback in the Barnum effect studies tends to attract higher ratings when presented as a whole as opposed to individual items (Layne 1978), therefore, in the present study, participants will be given their personality feedback sentence by sentence and asked to rate each statement for accuracy in order to avoid this.

The present study uses three types of personality feedback; neutral or vague feedback used in Forer's (1949) study, and the specific positive and negative feedback used by Furnham and Varian (1988). Specific rather than neutral positive and negative feedback statements were used in order to examine if there is a link between fraud susceptibility and acceptance of positive and negative feedback. Neutral positive and negative personality feedback may be more readily accepted by participants and may therefore not be suitable as a measure of susceptibility to fraud. For example, research found that victims of certain frauds may be more prone to flattery (Lea et al. 2009; Witty, 2013), therefore high ratings of specific positive items may provide an indicator of propensity for flattery.

In the previous study (Chapter 4) 'Compliance', a factor of Susceptibility to Fraud Scale, was found to have the largest part of the variance in fraud susceptibility. Therefore, the present study also utilised Gudjonsson's (1989) Compliance Scale (GCS) as an additional measure of concurrent validity for the STFS.

Since there is evidence that locus of control may be implicated in the acceptance of bogus personality feedback (Furnham, 1989; Snyder & Larson, 1972), the present study

included Sapp and Harrod's (1993) brief Locus of Control (LOC) measure in order to explore possible relationships with the STFS. Participants were also given their scores on the LOC measure after debriefing, to make reparation for deception.

Study 3 Research questions:

1. What is the nature of the relationship between susceptibility to fraud, compliance and locus of control? Are individuals who are more susceptible to fraud more compliant or more likely to assume external factors beyond their control as determining what happens in their lives?

2. Is susceptibility to fraud related to greater self-bias in responses to the Barnum type personality feedback? Are individuals who are more susceptible to fraud more likely to rate themselves higher than they rate others on neutral and positive items and lower on negative items).

3. Does the Barnum effect predict fraud victimisation? Do previous fraud victims show greater self- bias in relation to the Barnum effect?

5.2 Method

5.2.1 Participants

Participants were recruited by advertising the study on social media and participation was voluntary. No incentive was offered for participation apart from personality feedback, which was supplied at the end of the survey. The study was also advertised among first year undergraduate psychology students at the University of Portsmouth, who received a course credit for their participation, but who belonged to a different cohort to that recruited during Study 2. As the Barnum Effect paradigm relies on deception, participants were told that the purpose of this study was to help develop a new personality questionnaire, and allow the researcher to examine how people perceive the accuracy of feedback they receive about their personality characteristics from the test being developed.

Out of 531participants that started the survey, a total of 430 participants completed all parts of the survey, giving an attrition rate of 19%. Following debriefing, participants

were able to leave comments about the study. One participant requested for their data to be removed without an explanation and was removed from the data set. A further 4 participants were removed after leaving a comment saying that they suspected the feedback received had nothing to do with the measures they completed and one participant was removed due to scoring all the questions with the same score throughout the survey. The final sample of 424 participants consisted of 94 male and 330 female participants, 18 – 70 years of age (M =31.46, SD =12.91) out of which, 261were university students.

A total of 120 participants reported being defrauded in the past and 304 reported they have never been defrauded. Out of the 120 participants that have been defrauded, 47 stated that they reported the fraud to the authorities and 73 stated they did not report it.

The percentage of participants in the sample that reported they had been defrauded in the past varied across different age groups, the 18-25 years age group were the least likely to report being defrauded in the past (14%), compared to participants between the ages of 26 and 50 years (39%) or those between the ages of 51-70 years (49%).

5.2.2 Materials

The present study used Susceptibility to Fraud Scale (STFS), developed in the previous study (Chapter 4 and Appendix 1.6). The study also used the 9-item Brief Locus of Control (LOC) scale by Sapp and Harrod (1993), measuring internal locus of control, belief in chance and belief in powerful others, in order to measure the degree to which people feel they can control what happens to them. The inclusion of the Locus of Control scale in addition to being used to provide participants with some genuine personality feedback at the end of the study, also allowed the relationship between an individual's locus of control and fraud susceptibility to be examined. External locus of control may be characterised by feeling unable to control what happens which may indicate vulnerability to fraudulent offers, whilst a belief in powerful others may indicate those who succumb to authority cues in fraudulent communication. The Brief Locus of Control scale items can be found in Table 5.1.

Table 5.1
Sapp and Harrod (1993) Brief Locus of Control scale

Internal control α = .58	**Chance α = .65**	**Powerful others α = .72**
1. My life is determined by my own actions.	1. To a great extent, my life is controlled by accidental happenings.	1. People like myself have very little chance of protecting our personal interests where they conflict with those of strong pressure groups.
2. I am usually able to protect my personal interests.	2. Often there is no chance of protecting my personal interests from bad luck happenings.	2. My life is chiefly controlled by powerful others.
3. I can pretty much determine what will happen in my life.	3. When I get what I want, it is usually because I'm lucky.	3. I feel like what happens in my life is mostly determined by powerful people.

Since compliance was found to have the largest part of the variance in fraud susceptibility in the previous study, 20-item Gudjonsson (1989) Compliance Scale was included as a measure of concurrent validity for STFS. Gudjonson (1989) Compliance Scale items can be found in Table 5.2.

Table 5.2
Gudjonson (1989) Compliance Scale

Compliance Scale α = .71
1. I give easily to people when I am pressured.
2. I find it very difficult to tell people when I disagree with them.
3. People in authority make me feel uncomfortable and uneasy.
4. I tend to give in to people who insist that they are right.
5. I tend to become easily alarmed and frightened when I am in the company of people in authority.
6. I try very hard not to offend people in authority.
7. I would describe myself as a very obedient person
8. I tend to go along with what people tell me even when I know that they are wrong.
9. I believe in avoiding rather than facing demanding and frightening situations.
10. I try to please others.
11. Disagreeing with people often takes more time that it is worth.
12. I generally believe in doing what I am told.
13. When I am uncertain about things I tend to accept what people tell me.
14. I generally try to avoid confrontations with people.
15. As a child I always did what my parents told me.
16. I try hard to do what is expected of me.
17. I am not too concerned about what people think of me.*
18. I strongly resist being pressured to do things I don't want to do.*
19. I would never go along with what people tell me in order to please them.*
20. When I was a child I sometimes took the blame for things I had not done.

Note.
* Reverse item

Participants completed the STFS first, followed by the LOC scale and the Compliance Scale. To standardise the responses and make the questions appear as if they were part of the same measure, responses to all the scales were measured on a 5-point Likert scale by asking participants to indicate to what degree they agree with each statement (1 = Strongly disagree to 5 = Strongly agree). The range of scores for each subscale of the Sapp and Harrod (1993) LOC scale was therefore, 3 to 15. Higher scores indicate more internal locus of control, higher belief in chance and higher belief in powerful others.

The range of scores for the Gudjonson (1989) Compliance scale ranged from 20 to 100, with lower scores indicating lower compliance. The range of scores for the STFS total was from 26 to 130, with lower scores indicating lower susceptibility to fraud. Means, standard deviation and range of the scale scores found with the present sample are shown in Table 5.3.

Table 5.3
Means, standard deviation and range of the scale scores for the measures used in the experiment, $N = 424$

Measure	Minimum	Maximum	M	SD	Skewness
STFS	1.15	4.35	2.86	0.45	-.31
LOC internal	4.00	15.00	10.84	2.13	-.31
LOC chance	3.00	15.00	8.00	2.32	.12
LOC powerful others	3.00	15.00	7.40	2.68	.35
Compliance scale	26.00	92.00	57.49	12.76	-.17

5.2.3 Procedure

Participants were invited to participate in the study by advertising on different social media platforms and the university participant pool.

The invitation to participate gave the following information about the study:
"You are invited to take part in a research study looking into perceptions of accuracy of personality test feedback. The survey takes approximately 20-30 minutes and anyone over 18 is welcome to participate. You will first be asked to answer questions about your attitudes and daily activities, after which you will be presented with your personality feedback. Since we are trying to assess if the personality perception

questionnaire is accurate in delivering personality feedback, you will be asked to rate this feedback sentence by sentence on a 1-10 accuracy scale. "

The study was conducted using the online survey hosting software, Qualtrics. Participants were asked to complete the three psychometric questionnaires in the same order (STFS, LOC and Compliance), rating all questions on a 5- point Likert scale. After this, participants were told that they would be presented with their own personality feedback based on the psychometric measures they completed and that the feedback would be presented sentence by sentence in order to rate the quality of each feedback element.

They were asked to rate each statement for how accurate it is of them and also how accurate it was of people in general, using a 10-point semantic differential scale (with end descriptors of 1-not very accurate to 10- very accurate). After providing accuracy evaluations for each of the 21 personality statements, participants were asked if they experienced being defrauded in the past, if they reported it and how satisfied they were with any response from the authorities. As part of the debriefing process, participants were presented with the opportunity to share their views on the nature of the study and feelings regarding the deception used as well as being provided with details of further sources of support and information about fraud. Participants were also reminded of their right to request their data to be withdrawn from the study at this point. To make good on the study details given at the start of the questionnaire that participants would receive personality feedback after taking part in the study, all participants were automatically provided with their true personal score on the Locus of control scale together with an explanation what scores on this scale indicate, at the end of the survey.

5.2.4 Personality feedback

All participants received the same Barnum type personality feedback consisting of 7 positive, 7 negative and 7 neutral feedback statements (Collins, Dmitruk & Ranney, 1977; Forer, 1949; Furnham & Varian, 1988) but were told they were receiving their own personalised feedback to rate for accuracy (Table 5.4).

Table 5.4
Positive, negative and neutral Barnum type personality feedback

Positive Feedback	Negative Feedback	Neutral Feedback
1. You are often described by others as the most popular person they know.	1. In confrontation situations you tend to display extreme stubbornness and will not back down even when the evidence is stacked against you.	1. Security is one of your major goals in life.
2. Often you display the self-confidence and self-awareness that other people can only aspire to.	2. You have tendency to make unfavourable generalizations about people/situations of which you know nothing about.	2. While you have some personalit weaknesses, you are generally able to compensate for them.
3. You have such a broad spectrum of abilities that you could do almost anything in life.	3. You can be very patronizing to those you see as inferior to yourself.	3. At times you have serious doubt as to whether you have made the right decision or done the right thing.
4. You are very socially skilled and as such can cope with the most difficult situations with apparent ease.	4. When bored, you may often goad others into an argument just to "spice things up".	4. You prefer a certain amount of change and variety and become dissatisfied when hemmed in by restrictions and limitations.
5. You enjoy helping those who need it.	5. You are seldom constructively critical of your own actions.	5. At times you are extroverted, affable, sociable while at other times you are introverted, wary, reserved.
6. You inspire admiration and respect in all those you meet.	6. You do not suffer criticism in any form with good grace.	6. You have a great deal of unused capacity, which you have not turned to your advantage.
7. You have aesthetic interests and appreciate the really beautiful aspects of life.	7. You tend to overact or panic when in a stressful or potentially stressful situations.	7. Some of your aspirations tend to be pretty unrealistic.

5.3 Results

The primary objective of the analysis was to evaluate the ability of the newly developed STFS, to predict behavioural responses in a situation where participants received generalised personality feedback about themselves.

First, factor and reliability analyses of the newly developed STFS are presented, followed by the relationship between STFS and chosen psychometric measures, after which the results of the analyses on the acceptance of Barnum type feedback in relation

to STFS and previous fraud victimisation are presented. Finally, factors implicated in fraud reporting are considered.

5.3.1 Results of the factor and reliability analyses

Since the same sample was used to develop and test the reliability and validity of the STFS in Study 2 (Chapter 4), reliability analysis was repeated using the data from the present study. The factor with the highest reliability was Compliance (α=.87), followed by Decision Time (α=.70), Impulsivity (α=.60) and Vigilance (α=.57). Belief in Justice had the lowest reliability (α=.52), which is consistent with the results of the previous study, Study 2. Overall, the reliability of the STFS subscales was the same for Compliance, slightly higher for Decision Time and Belief in Justice and slightly lower for Impulsivity and Vigilance, when compared to results of the reliability analyses in Study 2 (Table 4.4).

To evaluate the item structure of the 26-item questionnaire, an exploratory factor analysis using principal axis factoring was conducted. Kaiser-Meyer-Olkin measure of sampling adequacy, 0.85 and Bartlett's test of sphericity (χ^2 (325) = 2850.9, p< .001) indicated that the data were suitable for factor analysis. A parallel analysis using Monte Carlo PCA indicated that only factors with a minimum Eigenvalue of above 1.48 should be retained, and inspection of the scree plot analysis suggested a point of inflection to occur in eigenvalues following the extraction of four factors (Pallant, 2013). Oblique rotation was used to determine factor composition. Initial item loadings for each of the five factors are shown in Appendix 1.7, Table 1.11. An exploratory factor analysis using principal components extraction, retaining Eigenvalues 1.48 and above, yielded similar results (Appendix 1.7, Table 1.12).

On the independent sample used in the present study, the factor structure of 4 out the 5 subscales was confirmed from Study 2. All questions were retained in their original parent factors for Compliance, Vigilance, Impulsivity and Belief in Justice, suggesting these factors are robust. However the stability of the Decision Time subscale could not be established from this sample, as it could not be distinguished from the Impulsivity subscale. This is something that further studies may want to evaluate.

5.3.2 Relationship between Susceptibility to Fraud scale (STFS), Gudjonson's (1989) Compliance scale, Sapp and Harrod's (1993) Locus of Control scale and age

In order to examine the relationships between the STFS scale with existing measures of psychology compliance and locus of control, Pearson correlations were calculated (Table 5.5). The STFS total score was positively correlated with Gudjonson's (1989) compliance scale, indicating that individuals who are more compliant may also be more susceptible to fraudulent messages. There was also a strong significant positive correlation between the STFS Compliance subscale and Gudjonson's Compliance scale, a measure of concurrent validity for this study. In addition, there was a significant positive correlation between the STFS Impulsivity subscale and a significant negative correlation between the STFS Vigilance subscale and Gudjonson's Compliance scale. This suggests that people who are more compliant are also more impulsive and less vigilant.

Table 5.5

Correlations between Susceptibility to Fraud scale (STFS), Gudjonson (1989) Compliance scale, Sapp and Harrod (1993) Locus of control scale (LOC) and age, *N* =424

	Gudjonson Compliance	LOC Internal	LOC Chance	LOC Powerful others	Age
STFS Compliance	.75**	-.30**	.42**	.43**	-.32**
STFS Vigilance	-.16*	.02	-.03	.05	.20**
STFS Impulsivity	.28**	-.09	.24**	.21**	-.25**
STFS Decision time	-.13	.12	-.22**	-.08	.15*
STFS Belief in justice	.02	.26**	-.01	-.11	-.10
STFS Total	.61**	-.19**	.38**	.30**	-.38**

Notes.
* p< .0016 (2 -tailed) Minimum accepted *p* value for statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 30).
** p< .001 (2-tailed).

Significant relationships were found between the STFS total and the three components of Sapp and Harrod's (1993) Locus of Control scale. Individuals who were more susceptible to fraud were also more likely to have external locus of control and showed greater belief in chance and the influence of powerful others. This may suggest that

individuals who may be more susceptible to fraud are more likely to believe that their life events are out of their control. They may also be more influenced by fraudulent communication, such as those pertaining to be from authority figures.

The STFS belief in justice also correlated positively with an Internal Locus of Control, indicating that people who believe in justice with regards to fraud, are more likely to believe they have autonomy and personal control over events in their life.

Significant relationships were also found between the STFS subscales and age suggesting that older participants reported a lower susceptibility to fraud, and seem to be less impulsive and less compliant. Older participants were also more vigilant and spent more time making decisions.

5.3.3 Susceptibility to fraud scale (STFS) and the acceptance of Barnum feedback as accurate of 'oneself' and 'other'

Overall, participants gave higher ratings to positive (*N=424, M* = 6.08, *SD* = 1.56) and neutral (*N=424, M* = 6.77, *SD* = 1.22), than negative items (*N=424, M* = 4.63, *SD* = 1.56), when asked to rate the items for how accurate they are of them. However, accuracy ratings differed for the same items when participants were asked to rate the items for people in general. Whilst the mean ratings were not that different for neutral items (*N=424, M* = 6.25, *SD* = .98), the accuracy ratings for positive items were lower (*N=424, M* = 5.60, *SD* = 1.06) and negative items were higher (*N=424, M* = 5.52, *SD* = 1.25) for people in general than when rating for 'oneself'. A comparison of mean accuracy ratings for each statement comparing self-assessments with people in general is shown in Table 5.6.

Personality feedback has been found to be regarded as more accurate when presented as overall feedback instead of individual statements (Layne, 1978). Presenting feedback sentence by sentence allows for deeper understanding on what statements may appear problematic for participants and enables more accurate analysis. For example statement 1 in Table 5.6 seems to be an anomaly as it seems to be rated as more accurate of others than oneself, which is not typically found for positive statements. Therefore, this particular statement may be more extreme than others: *You are often described by others as the most popular person they know*.
As such, it may be different to other positive statements.

Table 5.6
Mean accuracy ratings for positive, negative and neutral statements for 'oneself' and 'other', $N = 424$, df = 423

Feedback Statement	Self ratings M	SD	Other ratings M	SD	Mean difference	*t*	*p*
Positive							
1.	3.91	2.43	4.65	1.79	-0.75	-6.77	<.001
2.	5.68	2.50	5.55	1.68	0.13	1.10	.274
3.	5.73	2.51	5.28	1.75	0.45	4.05	<.001
4.	5.98	2.55	5.70	1.67	0.28	2.30	.022
5.	8.33	1.68	6.75	1.82	1.58	16.34	<.001
6.	5.60	2.26	5.28	1.67	0.32	3.64	<.001
7.	7.32	2.23	5.99	1.70	1.34	11.80	<.001
Total	6.08	1.56	5.60	1.06	0.48	7.00	<.001
Negative							
1.	5.04	2.70	5.69	1.91	-0.66	-5.59	<.001
2.	4.33	2.58	6.00	2.12	-1.67	-13.38	<.001
3.	4.21	2.67	5.36	2.19	-1.16	-9.23	<.001
4.	3.44	2.73	4.56	1.98	-1.12	-8.95	<.001
5.	4.88	2.75	5.61	1.89	-0.72	-5.46	<.001
6.	4.91	2.44	5.53	1.76	-0.62	-5.63	<.001
7.	5.63	2.96	5.91	1.78	-0.29	-2.15	.032
Total	4.63	1.56	5.52	1.25	-0.89	-12.67	<.001
Neutral							
1.	6.97	2.35	7.02	1.85	-0.05	-0.46	.649
2.	6.66	1.96	6.10	1.63	0.56	5.67	<.001
3.	6.97	2.32	6.08	1.85	0.89	9.03	<.001
4.	6.94	2.31	6.04	1.65	0.90	8.03	<.001
5.	7.89	2.41	6.32	1.95	1.57	14.31	<.001
6.	6.69	2.21	6.33	1.73	0.36	3.81	<.001
7.	5.29	2.80	5.85	2.08	-0.56	-4.89	<.001
Total	6.77	1.22	6.25	0.98	0.52	10.43	<.001

Correlations between subscales of the STFS and accuracy ratings for Barnum statements when rated for how accurate they are of 'oneself' are presented in Table 5.7. Overall, the STFS total score was positively correlated with negative Barnum feedback statements, suggesting that individuals who score higher on fraud susceptibility may more readily accept negative feedback about themselves. When examining the STFS subscale scores, those who scored higher on compliance and impulsivity were more likely to accept negative feedback. In contrast, individuals who take longer to make decisions and process information (STFS Decision Time subscale) assigned lower accuracy ratings to negative feedback. There was a significant negative correlation between positive Barnum statements when rated for 'oneself' and STFS Compliance, suggesting that more compliant individuals tended to rate positive feedback items as being less true of them. Additionally, there was a weak positive correlation between

STFS total and neutral Barnum statements, suggesting that more susceptible individuals were more likely to accept neutral or vague feedback as accurate descriptions of themselves.

Table 5.7
Correlations between Susceptibility to Fraud Scale (STFS) and type of feedback: positive, negative and neutral when rated for 'oneself'

	STFS Compliance	STFS Vigilance	STFS Impulsivity	STFS Decision time	STFS Belief in justice	STFS Total
Positive self	-.18**	.02	.06	-.08	.14	-.05
Negative self	.21**	-.07	.31**	-.23**	.07	.31**
Neutral self	.15	.10	.13	-.07	-.07	.10*

Notes.
* p< .0027 (2 -tailed) Minimum accepted *p* value for statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 18).
** p< .001 (2-tailed).

With regards to the mean accuracy ratings for feedback statements when asked how accurate they were for 'people in general', no significant relationships were found between any STFS subscales and ratings for positive statements.

Table 5.8
Correlations between Susceptibility to Fraud Scale (STFS) and type of feedback: positive, negative and neutral when rated for 'other'

	STFS Compliance	STFS Vigilance	STFS Impulsivity	STFS Decision time	STFS Belief in justice	STFS Total
Positive other	-.01	-.05	.11	-.09	.08	.07
Negative other	.15*	.05	.20**	-.09	.00	.15*
Neutral other	.08	.03	.14*	-.05	-.01	.09

Notes.
* p< .0027 (2 -tailed) Minimum accepted *p* value for statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 18).
** p< .001 (2-tailed).

There was a significant positive correlation between negative Barnum statements and STFS total, with those reporting higher susceptibility ratings being more likely to rate negative items as being more accurate of others. The same pattern was also observed for negative feedback with the STFS compliance and impulsivity subscales. A weak

positive correlation was also found between the STFS impulsivity subscale and mean accuracy ratings for neutral items when rated for 'people in general'.

Overall, the pattern of results between STFS subscales and the perceived accuracy of feedback may suggest some link between susceptibility to fraud and participants' interpretation of Barnum statements. Results suggest impulsivity and compliance were related to accepting negative feedback to be more accurate of both 'self' and 'other'. Compliant individuals also assigned lower accuracy ratings to positive items when applied to 'self' (but not others), suggesting that compliant individuals may be more likely to hold negative view of themselves.

5.3.4 Agreement frequencies for type of Barnum feedback and STFS

Whilst the mean accuracy ratings evaluated in the previous section, show the relative trend between the perception of feedback and fraud susceptibility, they do not provide an indication of the absolute degree to which participants accepted or did not accept feedback as true of them. In order to evaluate how many people accepted the feedback as accurate of them for each statement valence type, accuracy ratings of 7 or above (on the1-10 scale) were classified as agreement and statements with ratings below 7 as non-agreement. This provides an overview of whether the items were accepted as good descriptions of individual's personality or rejected (Table 5.9).

Table 5.9
Number of participants agreeing with positive, negative and neutral Barnum personality feedback statements

Total number of statements agreed with	**Positive**		**Negative**		**Neutral**	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
0	17	4.0	94	22.2	8	1.9
1	56	13.2	105	24.8	14	3.3
2	92	21.7	86	20.3	54	12.7
3	79	18.6	64	15.1	69	16.3
4	57	13.4	41	9.7	101	23.8
5	48	11.3	21	5.0	79	18.6
6	48	11.3	8	1.9	71	16.7
7	27	6.4	5	1.2	28	6.6
Total	424	100	424	100	424	100

Overall, people accepted a greater number of positive and neutral items as accurate descriptions of their personality than negative items. The neutral statements, in particular were accepted more readily, possibly due to their assumed high base rate in the general population: 66% of the participants agreed with 4 or more neutral statements, 42% agreed with 4 or more positive statements, whereas only 18% of the participants agreed with 4 or more negative statements.

The correlations between the Susceptibility to Fraud Scale (STFS) and the number of positive, negative and neutral Barnum feedback items that participants agreed with shown in Table 5.10, showed a similar general pattern of results as those found for accuracy ratings for 'self' (Table 5.7).

Table 5.10
Correlations between Susceptibility to Fraud Scale (STFS) and agreement frequencies for positive, negative and neutral Barnum personality feedback

	STFS Compliance	STFS Vigilance	STFS Impulsivity	STFS Decision time	STFS Belief in justice	STFS Total
Positive statements	-.14*	.05	.05	-.07	.12	-.05
Negative statements	.18**	-.03	.27**	-.20**	.04	.25**
Neutral statements	.10	.11	.13	-.04	-.07	.06
Overall statements	.05	.06	.20**	-.13	.04	.11

Notes.
* p< .0020 (2 -tailed) Minimum accepted *p* value for statistical significance (using Bonferroni adjustment for Type I error, 0.05 ÷ 24).
** p< .001 (2-tailed).

There was a significant positive correlation between the overall fraud susceptibility and the number of negative feedback statements that participants agreed with, indicating that those who were more likely to be susceptible to fraud were also more likely to accept negative statements as a genuine description of their personality. The same trend was also true for compliance and impulsivity, with individuals whom are more compliant and impulsive accepting a greater number of negative statements as accurate descriptions of their own personality.

A significant negative correlation was found between decision time and agreement with negative statements, indicating that those who take time making decisions and processing information accepted fewer negative statements as true descriptions of their personality. Additionally, there was a significant negative correlation between

compliance and acceptance of positive items, suggesting that compliant individuals were less likely to accept positive items as descriptions of their personality. The results also indicated a significant relationship between impulsivity and the total number of statements agreed with, suggesting more impulsive individuals were more likely to accept a greater number of feedback statements, of any valence, as being accurate descriptions of their personality.

5.3.5 Susceptibility to fraud and accuracy ratings for Barnum personality feedback for 'oneself' and 'other'

In order to examine differences in the pattern of acceptance of positive, negative and neutral feedback for people who differed in their level of susceptibility to fraud, high and low susceptibility to fraud groups were created using total scores on STFS.

The two groups were created using a median split of STFS total scores (low susceptibility group = 1- 2.92 and high susceptibility group = 2.92 - 5). This gave a total of 229 participants in the low susceptibility group and 195 participants in the high susceptibility group, whose perception of feedback was then evaluated separately for self-ratings of accuracy and accuracy with respect to people in general.

5.3.5.1 Ratings for self

A 3x2 mixed ANOVA with type of feedback (positive, negative, neutral) when rated for 'self' as a within-subject factor and fraud susceptibility (high, low) as a between-subject factor was conducted. Mauchly's test indicated that the assumption of sphericity had been violated for these data ($\chi^2(2)=35.80, p < .001$, W=.92), therefore the degrees of freedom were corrected using Greenhouse-Geisser estimates.

A significant main effect for valence of feedback (positive, negative and neutral) was observed ($F_{(1.85, 780.39)} = 343.72, p < .001, \eta^2_p = .449$) as well as for fraud susceptibility group ($F_{(1, 422)} = 6.37, p = .012, \eta^2_p = .015$). In addition, there was a significant interaction between feedback valence and fraud susceptibility on ratings of feedback accuracy when evaluated by participants as being true of themselves ($F_{(1.85, 780.39)} = 17.96, p < .001, \eta^2_p = .041$). The results indicate that the accuracy ratings for positive, negative and neutral Barnum statements differed between people in low and high susceptibility groups (Figure 5.1).

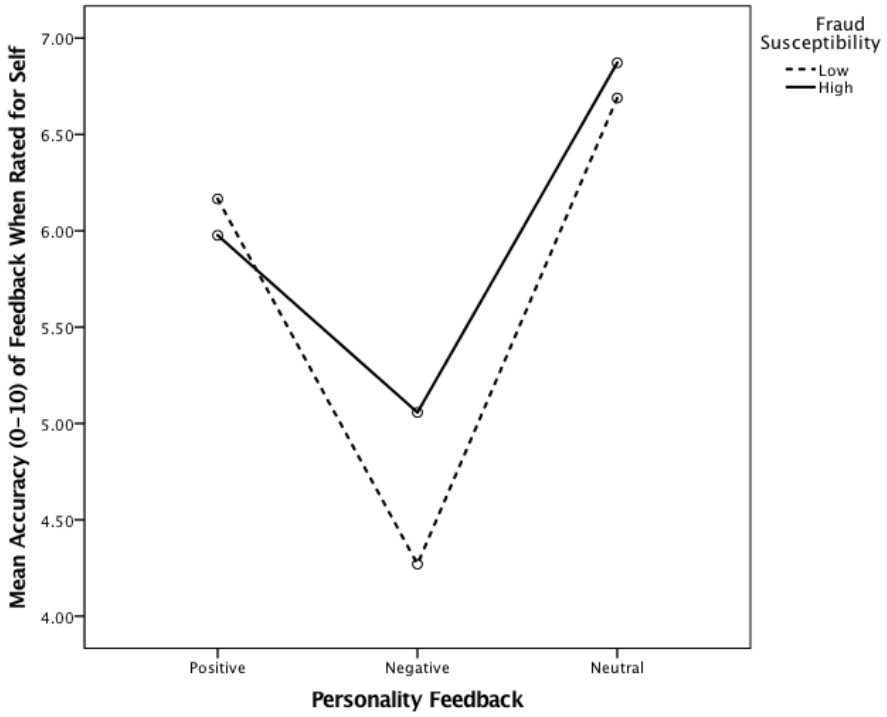


Figure 5.1 Accuracy ratings for personality feedback as true of 'oneself' for low and high fraud susceptibility groups

Pairwise comparisons using Bonferroni adjustment were used to examine differences in accuracy ratings between the high and low fraud susceptibility groups for each positive, negative and neutral feedback type. Results indicated a significant difference between high and low susceptibility groups with regards to negative feedback ($p < .001$), with participants in the high susceptibility to fraud group being more likely to rate negative Barnum feedback as true of themselves ($M = 5.06$, *95% CI* [4.84, 5.27]) than those in low susceptibility group ($M = 4.27$, *95% CI* [4.07, 4.47]).

No significant difference was found in mean accuracy ratings for positive feedback statements between low ($M = 6.12$, *95% CI* [5.97, 6.37]) and high ($M = 5.98$, *95% CI* [5.76, 6.20]) susceptibility groups ($p = .215$ *ns)*. Additionally, no significant difference was found in mean accuracy ratings for neutral statements between low ($M = 6.69$, *95% CI* [6.53, 6.85]) and high ($M = 6.87$, *95% CI* [6.70, 7.04]) susceptibility groups ($p = .125$ *ns)*.

These results suggest that more susceptible individuals are more accepting of negative feedback than less susceptible individuals whilst acceptance of positive and neutral feedback seems to not differ between the two groups.

5.3.5.2 Ratings for 'other'

A 3x2 mixed ANOVA with type of feedback (positive, negative, neutral) when rated for 'other' as a within-subject factor and fraud susceptibility (high, low) as a between-subject factor was conducted. Mauchly's test indicated that the assumption of sphericity had been violated for these data ($\chi^2(2)=70.34$, $p < .001$, W=.85) therefore the degrees of freedom were corrected using Greenhouse-Geisser estimates.

A significant main effect for type of feedback (positive, negative and neutral) was observed ($F_{(1.73, 731.45)} = 79.79, p < .001, \eta^2_p = .159$). The same was true for fraud susceptibility group ($F_{(1, 422)} = 6.88, p = .009, \eta^2_p = .016$), suggesting mean accuracy ratings when evaluated for 'others in general' differed depending on the type of feedback and participant's level of susceptibility to fraud. However, there was no interaction between type of feedback and fraud susceptibility for accuracy ratings for 'others' ($F_{(1.73, 731.45)} = .57, p = .540 (ns), \eta^2_p = .001$).

Pairwise comparisons using Bonferroni adjustment were used to examine differences in accuracy ratings between the high and low fraud susceptibility groups for each positive, negative and neutral feedback type.

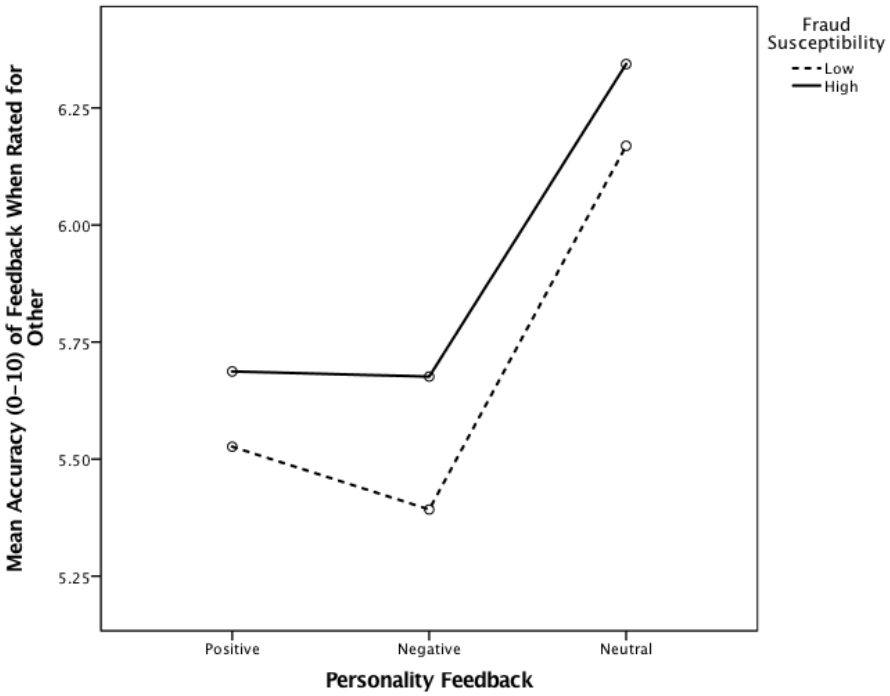


Figure 5.2 Accuracy ratings for personality feedback as true of 'other' for low and high fraud susceptibility groups

Results indicated a significant difference between high and low susceptibility groups with regards to negative feedback (p =.019), with participants in the high susceptibility to fraud group being more likely to rate negative Barnum feedback as true of others (M = 5.68, *95% CI* [5.50, 5.85]) than those in low susceptibility group (M = 5.39, *95% CI* [5.23, 5.55]).

No significant difference was found in mean accuracy ratings for positive feedback statements between low (M = 5.53, *95% CI* [5.39, 5.66]) and high (M = 5.69, *95% CI* [5.54, 5.84]) susceptibility groups (p = .120 *ns)*. Additionally, no significant difference was found in mean accuracy ratings for neutral statements between low (M = 6.17, *95% CI* [6.04, 6.30]) and high (M = 6.34, *95% CI* [6.21, 6.48]) susceptibility groups (p = .069 *ns)*.

These results suggest that more susceptible individuals are more critical of others than less susceptible individuals. The ratings of positive and neutral feedback did not differ between the two groups.

5.3.6 Susceptibility to fraud scale (STFS) and self-bias in response to Barnum personality feedback

Previous Barnum effect studies have found that participants assign higher scores to themselves on neutral and positive statements than compared to when asked to rate how applicable the same statements are to people in general, whilst for negative items, this pattern is reversed (Dana & Fouke, 1979; Davis 1997; Furnham &Varian, 1988; Layne, 1978). In her interview study with victims of fraud and those who reported receiving but not responding to fraudulent offers, Cross (2013) found that fraud victimisation is often blamed on the victim's decision to respond and engage with fraudulent schemes, even in situations where there is evidence that the scam was highly sophisticated. This may indicate that those who managed to avoid being defrauded in the past feel they are better at recognising fraudulent practices in general.

In order to examine the extent to which participants recognise that the bogus feedback provided in this study could also be applicable to other people (i.e. to what extent they evaluated feedback accuracy for themselves as being different from others) and whether this would be related to fraud susceptibility, difference scores were created. This was done by calculating the difference between the accuracy scores participants attributed to

themselves and those they assigned to others for each of the 7 different positive, negative and neutral Barnum feedback statements.

A difference value of zero would indicate that the individual feels they are no different to others, whereas a positive value indicates they evaluate themselves more highly than others and a negative value indicates they evaluate others more highly than themselves on the attribute under evaluation. Mean (self - other) difference scores were then calculated for each participant for the 7 statements relating to each feedback valence type and compared between high and low fraud susceptibility groups.

A 3x2 mixed ANOVA with type of feedback (positive, negative, neutral) as a within-subject factor and fraud susceptibility (high, low) as a between-subject factor was conducted on the difference scores (self-other). Mauchly's test indicated that the assumption of sphericity had been violated for these data ($\chi^2(2)=76.37, p < .001$, W=.83), therefore the degrees of freedom were corrected using Greenhouse-Geisser estimates.

A significant main effect was found for type of feedback (positive, negative and neutral) for difference scores ($F_{(1.72, 723.90)} = 188.97, p < .001, \eta^2_p = .309$). Mean difference scores for each feedback valence type are shown in Figure 5.3.
Positive ($M = .46$, *95% CI* [.33, .60]) and neutral ($M = .52$, *95% CI* [.43, .62]) statement difference scores had positive mean values, indicating people felt these were more accurate of themselves than others. However, negative statements had negative mean difference scores ($M = -.87$, *95% CI* [-1.01, -.73]), suggesting participants thought these tended to be more accurate of other people as opposed to themselves.

The main effect for fraud susceptibility group (high and low) was not significant ($F_{(1, 422)} = 0.401, p = .527$*(ns)*$, \eta^2_p = .001$), however a significant interaction was observed between fraud susceptibility and type of feedback ($F_{(1.72, 723.90)} = 13.93$, $p < .001, \eta^2_p = .032$). Whilst both, low and high fraud susceptibility groups rated themselves as similar to others on neutral Barnum statements, the high susceptibility to fraud group had lower mean difference scores for positive feedback statements, but higher mean difference scores for negative statements than the low susceptibility to fraud group (Figure 5.3).

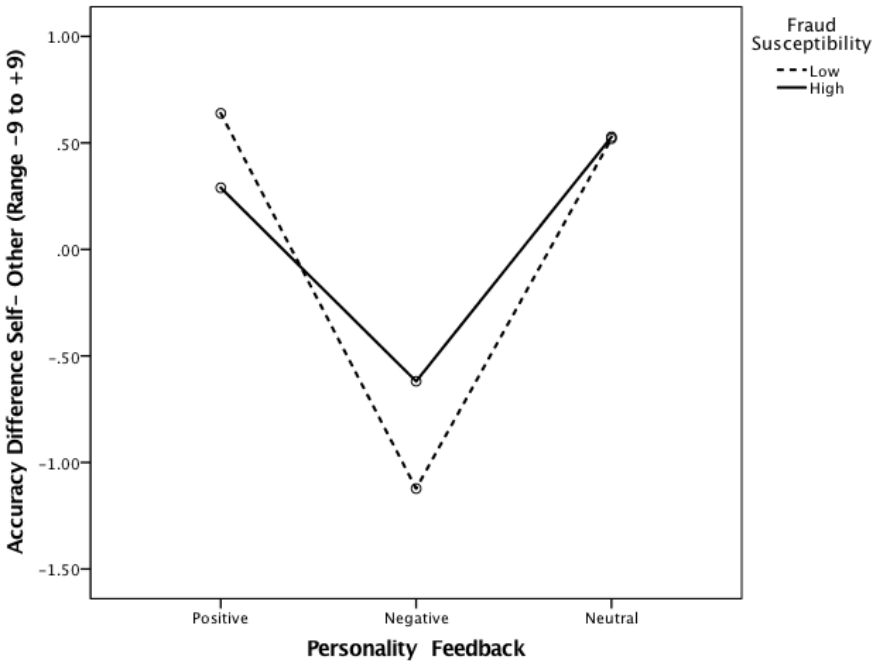


Figure 5.3 Personality feedback accuracy ratings difference (self – other) for low and high fraud susceptibility groups

This suggests that those in the high susceptibility group were less likely to see themselves as superior to others than those in low susceptibility group (i.e. high susceptibility individuals reported negative feedback as more true of them, and reported themselves as being broadly similar to others with respect to neutral feedback items).

Pairwise comparisons using Bonferroni adjustment were used to examine difference scores between the two fraud susceptibility groups for each type of positive, negative and neutral feedback statements.

The results for positive feedback statements suggest there was a significant difference between the high and low susceptibility groups ($p = .011$). Individuals in the high susceptibility group were less likely to view themselves as superior to others ($M = .29$, *95% CI* [.09, .49]) than those in the low susceptibility group ($M = .64$, *95% CI* [.46, .82]).

The results for negative feedback statements suggest there was a significant difference between the high and low susceptibility groups ($p < .001$). Individuals in the high susceptibility group were more likely to view others as superior to them ($M = -.62$, *95% CI* [-.82, -.42]), than compared to the low high susceptibility group ($M = -1.12$, *95% CI*

[-1.31, -.94]). Taken together, these findings may suggest that people whom exhibit high susceptibility to fraud are less likely to regard themselves as superior to others.

There were no differences between the high susceptibility to fraud group (M = .53, *95% CI* [.38, -.67]) and low susceptibility to fraud group (M = .52, *95% CI* [.39, -.66]), with respect to their interpretation of neutral feedback (p = .937), with the confidence intervals for both groups suggesting they did not regard themselves as different from others.

5.3.7 Fraud victimisation and the acceptance of Barnum personality feedback

To examine whether responses to Barnum personality feedback statements differentiated between those who had or had not previously been a victim of scams, the evaluation of self vs other difference scores for the positive, negative and neutral Barnum feedback was extended to consider scam victimization. In the present sample, a total of 120 participants reported being defrauded in the past and 304 reported they have never been defrauded.

A 3x2 mixed ANOVA with type of feedback (positive, negative, neutral) as a within-subject factor and fraud victimisation (defrauded, never defrauded) as a between-subject factor was conducted on difference scores (self-other). Mauchly's test indicated that the assumption of sphericity had been violated for these data ($\chi^2(2)=85.51, p < .001$, W=.82), therefore the degrees of freedom were corrected using Greenhouse-Geisser estimates.

A significant main effect for type of feedback was found ($F_{(1.69, 712.95)} = 167.32$ $p < .001, \eta^2_p = .284$). The main effect of fraud victimisation (defrauded, never defrauded) was not significant ($F_{(1, 422)} = 0.34$ $p = .563$*(ns)*, $\eta^2_p = .001$), however a significant interaction between type of feedback and scam victimisation was found ($F_{(1.69, 712.95)} = 4.33, p = .019, \eta^2_p = .010$). Mean difference scores for each fraud victimisation group are shown in Figure 5.4, for each type of feedback statement.

Pairwise comparisons using Bonferroni adjustment were used to examine difference scores for those that had been defrauded in the past and those that have never been defrauded, for each type of positive, negative and neutral feedback.

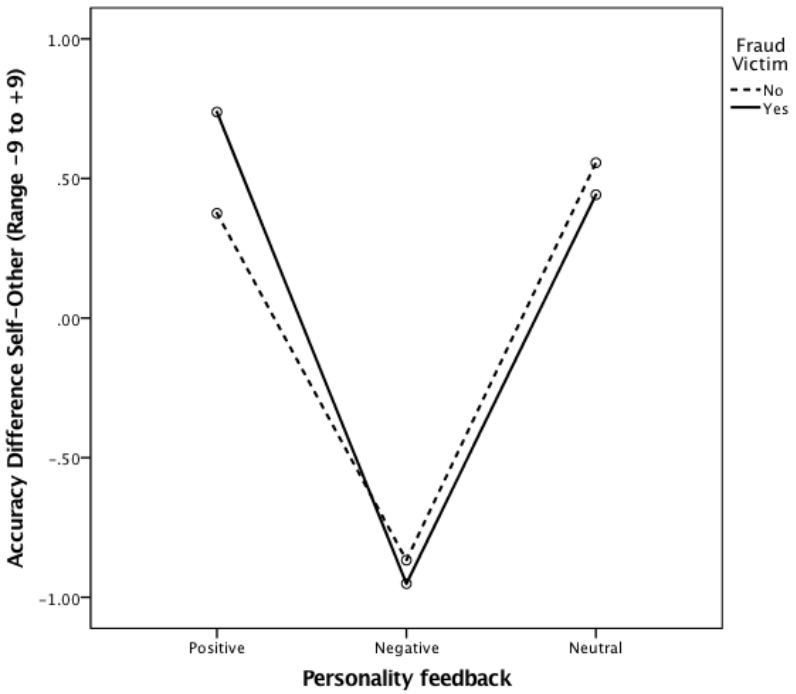


Figure 5.4 Personality feedback accuracy ratings difference (self – other) for previous fraud victims and non-victims

Results suggested there was a significant difference between the scam groups with respect to their evaluation of positive feedback (p = .017). Individuals that reported being defrauded in the past were more likely to view themselves more favourably than others (M = .74, *95% CI* [.49, .99]) compared to those that had never been defrauded (M = .38, *95% CI* [.22, .53]).

There were no differences between the two groups in their evaluation of negative Barnum statements. Individuals that reported being defrauded in the past (M = -.95, *95% CI* [-1.21, -.69]) did not differ from those whom reported they had never been defrauded (M = -.87, *95% CI* [-1.03, -.70]). The same trend was found for neutral items. Those that reported being defrauded (M = .44, *95% CI* [.26, .63]) did not differ from those that have never been defrauded (M = .56, *95% CI* [.44, .67]).

Together these results suggest that fraud victims may regard themselves as considering positive qualities to be a more accurate description of themselves than others, compared to non-victims, but that they do not differ in their interpretation of the accuracy of negative or neutral feedback compared to non-victims.

5.3.8 Susceptibility to fraud and previous fraud victimisation

Independent-samples t-tests were conducted to compare those who have never been fraud victims and those that reported being defrauded in the past. Based on this initial analysis, only one significant difference was found with previous victims of fraud scoring lower than non-victims on the Belief in Justice scale, suggesting that fraud victimisation influences one's perceived view of justice (Table 5.11).

Table 5.11
Comparison of groups 'Non-victim' (*N*=304) and "Previous fraud victim' (*N*=120) and the subscales of Susceptibility to Fraud Scale using independent samples t-tests (422 df)

Subscale	Non-Victim		Previous Fraud Victim		*t*	*p*	Cohen's *d*
	Mean	*SD*	*Mean*	*SD*			
Compliance	3.16	0.80	3.03	0.84	1.53	.13 ns	0.16
Vigilance	3.64	0.65	3.73	0.63	-1.29	.20 ns	-0.14
Impulsivity	3.21	0.75	3.26	0.71	-0.72	.47 ns	-0.07
Decision time	3.54	0.76	3.49	0.75	0.58	.56 ns	0.07
Belief in justice	2.98	0.63	2.82	0.74	2.19	.029	0.23

Given that prior exposure to risk will not be the same for younger and older participants, and the fact that non-victims (M = 29.00, SD = 12.33) were found to be significantly younger than previous victims of fraud (M = 37.68, SD = 12.28); t(422) = -6.54, p <.001), the comparison of STFS subscales between victims and non-victims was repeated whilst controlling for participants' ages. Independent groups analysis of covariance (ANCOVA) was used to compare the two groups, with age as a covariate (Table 5.12).

Table 5.12
Comparison of groups 'Never scammed' (*N*=304) and "Scammed once or more' (*N*=120) and the subscales of Susceptibility to Fraud Scale using one-way ANCOVA with age as a covariate (1,421 df)

Subscale	Non-Victim			Previous Fraud Victim			*F*	*p*	Partial eta-square
	Adjusted Mean	95% CI Lower	Upper	Adjusted Mean	95% CI Lower	Upper			
Compliance	3.11	3.02	3.20	3.16	3.01	3.30	0.27	.60ns	.001
Vigilance	3.66	3.59	3.74	3.67	3.55	3.78	0.01	.97ns	.000
Impulsivity	3.17	3.09	3.25	3.37	3.24	3.50	6.34	.012	.015
Decision time	3.56	3.48	3.65	3.43	3.29	3.57	2.63	.11ns	.006
Belief in justice	2.97	2.89	3.04	2.85	2.72	2.97	2.69	.10ns	.006

After adjusting for age, a significant difference was found between victims and non-victims with respect to Impulsivity, with previous victims of fraud being more impulsive than non-victims. However, the effect of the Belief in justice was no longer significant.

5.3.9 Factors involved in fraud reporting

Out of 120 participants that reported being defrauded in the past, 47 stated they have reported the crime to the authorities and 73 stated they did not. In order to explore differences in the attributes of those who do and do not report fraud independent samples t- tests were conducted comparing the two groups on each of the key dependent measures evaluated in the present study (Table 5.13).

Table 5.13
Personality differences among fraud victims that reported (*N*=47) and those that did not report (*N*=73) the victimisation (118 df)

Measure	Reported		Did not report		*t*	*p*	Cohen's *d*
	Mean	SD	Mean	SD			
STFS Compliance	2.85	0.83	3.15	0.82	-1.94	.055*ns*	-0.36
STFS Vigilance	3.78	0.59	3.70	0.65	0.70	.48*ns*	0.08
STFS Impulsivity	3.12	0.79	3.36	0.64	-1.78	.078*ns*	-0.33
STFS Decision time	3.51	0.78	3.36	0.73	0.22	.83*ns*	0.20
STFS Belief in Justice	2.66	0.80	2.92	0.68	-1.94	.055*ns*	-0.35
STFS Total	2.68	0.53	2.89	0.46	-2.20	.030	-0.42
Gudjonson Compliance	53.68	12.83	59.49	12.09	-2.08	.040	-0.47
LOC Internal	11.26	2.15	11.04	2.03	0.55	.58*ns*	0.11
LOC Chance	7.47	2.62	8.19	2.31	-1.55	.12*ns*	-0.29
LOC Powerful others	6.57	2.95	8.03	2.37	-2.97	.004	-0.55
Barnum positive DT	0.89	1.47	0.64	1.38	0.95	.35*ns*	0.16
Barnum negative DT	-1.20	1.86	-0.79	1.40	-1.38	.17*ns*	-0.25
Barnum neutral DT	0.53	1.41	0.39	1.04	0.62	.54*ns*	0.11

Note.
DT = Difference Total

There was a significant difference in SFTS total scores between those who did and did not report the fraud, with those who had higher susceptibility scores being less likely to report the fraud.

A similar trend (to STFS total) was observed for the STFS Compliance and Belief in Justice subscales, with those who did not report the fraud being more compliant and more likely to believe in justice, than those who did not report the fraud, although these effects marginally failed to reach statistical significance (p=.055)

With regards to Locus of control scale, a significant difference was found between those who reported and did not report being defrauded, with respect to their belief in powerful others. Individuals who did not report being defrauded were more likely to believe in powerful others, than those who did report the fraud. No other personality differences were observed between fraud reporters and non-reporters, and no differences in the interpretation of Barnum feedback were found between fraud reporters and non-reporters.

5.4 Barnum Study Discussion: Study 3

The present study sought to establish whether people who are more susceptible to fraud, as indicated by their responses to the STFS would be more inclined to exhibit stereotypical Barnum effect responses (i.e. being more accepting of positive and neutral feedback and rejecting negative feedback) than those who are less susceptible.

The present study was conducted using an online survey, in order to collect the responses to psychometric measures and feedback ratings at the same time, minimising attrition (also Cupperman et al., 2014). Studying the Barnum effect typically involves deception, which has ethical implications. Using the survey method ameliorated some of the ethical implications, as the participants were given their personal scores on one of the measures they completed at the end of the survey, which is something they were promised at the beginning of the study. In the past, studies have tested if personality feedback would be rated differently when provided in oral rather than written form (Snyder & Shenkel, 1976), computer generated as opposed to interpreted by an expert (Fletcher et al., 1996) with no differences reported. Therefore, studies wishing to utilise

the Barnum effect paradigm may find that using an online survey is a good way to collect responses at the same time and offer participants bona-fine personality feedback they were promised, minimising potential harm.

In the present study, the Barnum effect was able to differentiate between previous fraud victims and non-victims as well as low and high susceptibility groups, although not in the way the study predicted. Nevertheless, it is suggested that the Barnum effect may be a used as a measure of fraud susceptibility.

Comparing previous fraud victims to non-victims, the present study found that fraud victimisation influences one's perceived view of justice, with greater belief in justice reported by non-victims. After controlling for age, the results indicated that previous fraud victims tend to be more impulsive, however, the effect of Belief in Justice was no longer significant.

5.4.1 Susceptibility to fraud and the Barnum effect

Overall, the ratings of the Barnum type personality feedback followed the expected pattern. Positive and neutral personality statements were accepted as more accurate of oneself and negative items as less accurate, suggesting that the experimental procedure used was successful in invoking the Barnum effect. However, individuals that were more susceptible to fraud were more likely to assign higher accuracy ratings to negative items when rating the accuracy of feedback for oneself, than those in the low susceptibility group. They also assigned higher accuracy to negative items when rating the same feedback for how applicable it is to people in general, than low susceptibility group. These results suggest that individuals that are more susceptible to fraud may be more self-deprecating. Instead of viewing those that exhibit susceptibility to fraud as gullible, they may be seen as more self-critical, as they are aware of their flaws.

When it came to difference scores (self-other), calculated in order to measure self-bias (i.e. the degree to which participants felt they were better or worse than people in general), individuals in the high susceptibility group were less likely to see themselves as superior to others than those in low susceptibility group. These results suggest that the hypothesis, that individuals more susceptible to fraud will be more likely to see themselves as superior to others, is rejected.

The results suggested that there may be a link between the subscales of the STFS and the perceived accuracy of the personality statements, with more compliant and impulsive individuals rating negative personality feedback as more accurate of both 'self' and 'other'. Those that take time to consider their decisions agreed with fewer negative statements. Additionally, individuals who were more impulsive were also more likely to accept a greater number of feedback statements as accurate descriptions of their personality, irrespective of valence, which may suggest that, in a situation that could be a scam, they may be less likely to scrutinise information given to them.

As well as rating the negative feedback as more accurate of themselves and others, compliant individuals also assigned lower accuracy ratings to positive items when rating the feedback for oneself but not for others. These results suggest that compliant individuals may have a more negative perception of themselves. This is consistent with previous research, which found a positive relationship between compliance and low self-esteem, as well as state and trait anxiety, paranoia and suspiciousness (Gudjonsson, Sigurdsson, Brynjólfsdóttir & Hreinsdóttir, 2002). Furthermore, Gudjonsson, et al. (2002) posit that compliant individuals may disagree with things they consciously decide to go along with and as such, compliance is different to suggestibility. Additionally, Cialdini and Goldstein (2004) argue that compliant individuals are aware they are being encouraged to respond in a certain way. Taken together, the results could suggest that compliant individuals may be more susceptible to fraud even in cases where they are aware the situation they found themselves in is harmful to them and feel they have no control. This realisation may be responsible for feelings of low self-esteem and the way they view themselves, therefore the acceptance of negative Barnum type personality feedback in compliant individuals may be down to low self-esteem. Additionally, research by Fischer et al., (2013) found a negative association between compliance and feelings of superiority and suggested that this might be down to fraud victimisation leading to erosion of self-worth. This may in part, explain the findings, that people who are more susceptible to fraud feel they are inferior to others.

The present data may also help to explain some of the findings in the first study, as some participants reported being targeted at times when they were down and their self-esteem was already suffering. Compliance may further exacerbate this. Mosher (1965) found that participants with higher scores on Marlowe Crown scale, which measures social desirability, were more likely to accept negative feedback. Therefore, the

acceptance of negative items may be a unique feature of individuals that are more compliant or eager to please and therefore, more susceptible to persuasion by others.

5.4.2 Previous fraud victimisation and the Barnum effect

The present study found that participants that reported being defrauded in the past rated positive feedback as more accurate of themselves than of others, than non-victims did, suggesting they hold a more favourable view of themselves than they do of others. No differences were found for negative and neutral items, therefore the hypothesis that the Barnum effect would predict previous fraud victimisation was supported, but only in part. These findings regarding the victims of fraud having an overly positive view of self may mean they may be prone to flattery. For example, previous research found that proneness to flattery could be exploited by scammers (Lea et al., 2009; Whitty, 2013). Therefore, overly positive view of self may indicate vulnerability to fraud in certain fraudulent situations.

These findings were somewhat surprising, as it was expected that susceptible individuals would show the same pattern as victims of fraud, be more 'gullible' and more likely to fall for the Barnum effect (i.e. assigning higher ratings to positive items and lower ratings to negative items) than less susceptible individuals. In contrast, it seems that susceptible individuals are more self-deprecating. One explanation for these results may be that those previously defrauded may not be susceptible to fraud. For example, frauds differ in the amount of cooperation they require from the victim from none to quite extensive cooperation (Titus and Gover 2001). Victims of ID fraud often have no communication with the scammer; therefore, their victimisation may not be down to individual characteristics. Scammers may steal documents or cards of the victim and use them for fraudulent activities (Button et al., 2009a). Frauds also differ in how plausible and credible they appear. For example, highly sophisticated frauds, such as spear phishing attacks can be very convincing due to the amount of effort the scammer may put in sourcing specific information about the victim, in order to deceive (Parmar, 2012), therefore they may affect individuals that would not otherwise be vulnerable to fraud. Other types of fraud, such as making a purchase online from what seems like a legitimate business and not receiving the goods paid for, also may not indicate individual's susceptibility to fraud but may end in fraud victimisation. This was evident in the fact that some of those who self-reported being defrauded in the past were in the low susceptibility group. Although participants were asked about prior

victimisation, the study failed to enquire about the details of the fraud that took place. This information may have provided an insight into why previous fraud victims responded differently to the Barnum type feedback than individuals susceptible to fraud. Another reason for these results could be that some previous fraud victims changed their behaviour or attitudes after being defrauded, making them less susceptible to fraud as a result.

It is also possible that individuals in the high susceptibility group may be aware of their susceptibility and were able to avoid being defrauded as a result. As younger individuals were more likely to be susceptible to fraud, and given the fact that fraud victims in this study tended to be older, previous victimisation may be down to the number of fraudulent offers received across one's lifespan, with younger participants less likely to receive as many fraudulent offers as those that are older.

5.4.3 Personality factors in susceptibility to fraud

Greater fraud susceptibility was positively related to Gudjonson's (1989) Compliance (GCS) scale (a measure of concurrent validity), as was Compliance, a subscale of STFS. Additionally, compliant individuals were also more impulsive and less vigilant. The results suggest that individuals who are more susceptible to fraud may be more likely to accede to the will of others.

Previous studies (Cupperman et al., 2014; Furnham, 1989; Snyder & Larson, 1972) have found a link between the acceptance of bogus personality feedback and an external locus of control, therefore a Locus of Control measure (Sapp & Harrod, 1993) was used in order to examine the relationship between STFS and locus of control. Individuals who were more susceptible to fraud were more likely to have an external locus of control (i.e. believe that their life events are out of their control), as did compliant individuals. They were also more likely to believe in powerful others and chance, which means that they may be more influenced by authority cues in fraudulent communication or more likely to believe that luck in on their side, which could be exploited by various scams (e.g. fake lotteries or free prizes).

The results also indicated that individuals, who believe in justice with regards to fraud, were more likely to have an internal locus of control. However, as previous fraud

victimisation was found to influence one's perceived view of justice, these results may mean that perceived control over one's life changes following fraud victimisation.

5.5 Future considerations

The present study is the first research study to use the Barnum effect as a measure of fraud susceptibility. Although it was predicted that participants with higher scores on the STFS would exhibit the same pattern of Barnum type feedback acceptance as previous fraud victims, this was not the case. Participants that were more susceptible to fraud were more likely to accept negative feedback as true descriptions of their own personality, and this was especially true of more compliant and impulsive individuals. However, the opposite was true for previous fraud victims, who were more likely to accept positive statements as true descriptions of their personality. One possible reason for this disparity may be that some fraud victims may not be susceptible to fraud, which could be down to becoming more vigilant following fraud victimisation. Another possible reason for these results is that while some people may be more susceptible to fraudulent offers, they may be aware of it and are able to compensate for this. This was observed in an interview study, Study 1 in this programme of research, where one of the participants reported being aware of his inability to say no, due to which he devised a strategy to protect himself from situations that may exploit this.

Due to low participant numbers, the interaction between susceptibility, victimisation and the acceptance of differently valenced personality feedback could not be observed, therefore future studies may wish to replicate the study addressing this limitation.

Future studies may also wish to ask participants to report details of previous victimisation, in order to examine if fraud susceptibility varies across different types of frauds and length of communication with the scammer (i.e. identity fraud versus scams that require lengthy communication or greater cooperation with the scammer) and how this may impact acceptance of Barnum type personality feedback. Additionally, future studies may also want to examine the role of self-esteem and fraud susceptibility, especially with regards to compliance and the acceptance of the negative feedback.

The present study was seen as an opportunity to test the reliability of the STFS on an independent sample. Results of the reliability analysis indicated reliability of the Compliance scale to be exactly the same as in Study 2 (Chapter 4). However, reliability of the Decision Time subscale was higher, while the reliability of Vigilance and Impulsivity subscales was lower in the present study. Although reliability for Belief in Justice was higher than in Study 2, its reliability was still relatively low (α=.57) and it remained the least reliable factor.

The results of the factor analysis indicated that the factor structure of four out the five scales was confirmed from the previous study, Study 2; Compliance, Vigilance, Impulsivity and Belief in Justice. This suggests that those factors may be reasonably robust. However the stability of the Decision Time subscale could not be established from this sample due to the fact that it could not be distinguished from the Impulsivity subscale. Therefore, future studies may wish to evaluate the robustness of the STFS subscales, especially Belief in Justice, which did not yield any interesting results in the present study. Due to the low reliability of this factor, it would be of value for future studies to either develop it further or omit it from the scale.

5.6 Conclusion

In the present study, the Barnum effect paradigm was used to explore its potential as a measure that could be used to differentiate between victims and non-victims of fraud, in order to examine its applicability as a tool for assessing the predictive validity of the newly developed STFS scale. As such, the present study was the first to use the Barnum effect as a proxy scam situation. The Barnum effect predicted previous fraud victimisation, with those previously defrauded being more likely to accept positive Barnum type feedback items as accurate descriptions of their personality than non-victims, indicating possible propensity to flattery. Although the study yielded conflicting results; those susceptible to fraud were more likely to rate negative Barnum type feedback items as accurate descriptions of their personality than those who were less susceptible, whilst previous fraud victims rated positive items as more accurate than non-victims, possible explanations for this have been put forward. Despite this, the present study was able to contribute new knowledge to research utilising the Barnum effect paradigm, specifically that high susceptibility to fraud, as measured by the

Susceptibility to Fraud Scale is connected to the acceptance of the negatively valenced Barnum type feedback items. Additionally, individuals in the high fraud susceptibility group were more likely to view others as superior to them than those in the low fraud susceptibility group and were less likely to report fraud victimisation to the authorities, which may be down to the self-deprecation. By asking participants to rate each feedback statement for accuracy, instead of presenting the feedback as a whole, the present study was able to identify that individuals with higher scores on the STFS Impulsivity subscale were more likely to agree with any feedback, irrespective of valence. This suggests that asking participants to rate the feedback by evaluating each statement instead of an overall feedback may be more effective in measuring agreement with Barnum type feedback.

Chapter 6

General discussion

6.1 Introduction to general discussion

This chapter presents a discussion of the research findings in this thesis. First, aims and rationale for the research are presented, followed by short summaries of the three studies forming the programme of this research. Summary of the research findings are presented and discussed next. The implications of this research are presented, including the recommendations for future research. Finally, limitations of this research are outlined.

6.2 Aims and rationale for the research

Annual Fraud Indicator figures for recent years suggest that fraud is on the rise (Table 2.1, Chapter 2). Current fraud prevention measures are not always effective, however, there is an opportunity to learn from the victims of fraud, learn about the complexity of fraudulent situations, scam correspondence, persuasion techniques and persuasive lures that scammers are good at designing. But is it enough? Scam prevention measures are frequently ignored because of their abundance, especially online (Egelman et al., 2008; Frauenstein & Flowerday, 2016; Furnell & Thompson, 2009). There is evidence that security and privacy attitudes may be down to individual differences and that designing security warnings that address users' individual characteristics may be beneficial (Egelman & Peer, 2015). This may also be the case for other fraud warnings. While scammers are getting increasingly smarter, targeting specific victims, exploiting specific human attributes, fraud prevention is yet to start considering individual differences in the fight against fraud. This programme of research set to investigate individual characteristics in vulnerability to fraudulent offers and to create a valid and reliable psychometric measure that would be able to pinpoint potential areas of vulnerability to fraud. The research expands on the research of Modic and Lea (2012, 2013) exploring susceptibility to persuasion and its relation to scam compliance.
In order to do this, three separate studies were conducted:

(i) Identify factors and personal attributes that may contribute to making judgment errors in scam situations by conducting interviews with victims and near victims of fraud (Study1, Chapter 3).

(ii) Construct and develop a psychometric questionnaire designed to indicate an area of individual susceptibility to fraudulent offers (Study 2, Chapter 4).

(iii) Test the utility of the newly developed measure of fraud on a proxy scam situation (Study 3, Chapter 5).

6.3 Summary of research studies

6.3.1 Interview study: Study 1

The first study in this programme of research, described in Chapter 3, explored the scam process, through the narratives of fraud victims, taking care to also consider the present circumstances of each victim. Through the participants' stories, three distinct stages of a scam process emerged, each with its own themes and subthemes, relevant to understanding the nuances of fraud victimisation, fraud reporting and the psychological impact on victims. Interviews have been found to be an effective way of gathering data on the topic of fraud, which can be used in variety of ways (Button et al., 2013; Cross, 2013, 2015; Fischer et al., 2013; Lea et al., 2009; Olivier et al., 2015; Whitty, 2013). The analytical approach was based on thematic analysis (Braun & Clarke, 2006).

6.3.2 Scale development study: Study 2

Chapter 4 describes the stages involved in the development of the Susceptibility to Fraud Scale (STFS). The first stage was based on the findings of the previous study, Study 1, as well as previous research looking into susceptibility to persuasion and errors in judgments (Lea et al., 2009; Modic & Lea, 2012, 2013), theoretical models of Gullible Action and Foolish Action (Greenspan, 2008, 2009) and the Model of Scamming Vulnerability (Langenderfer & Shimp, 2001). In this stage, a pool of questionnaire items was generated and tested by asking a range of content experts to rate each question for applicability to fraud and provide feedback. The chosen questionnaire items were distributed to participants via an online survey in the second stage of the study, along with examples of genuine and phishing email correspondence, Modic and Lea's (2013) Susceptibility to Persuasion scale and hypothetical scam scenarios (Modic & Lea, 2012). An exploratory factor analysis using principal component extraction was conducted in order to identify the number of factors in the data. The final scale yielded five subscales of susceptibility to fraud; Compliance, Implusvity, Vigilance, Decision time and Belief in justice. The newly developed

measure was tested against examples of genuine and phishing email correspondence and hypothetical scam scenarios.

6.3.3 The Barnum effect study: Study 3

In the final study in this programme of research, the utility of the scale was tested using the Barnum effect as a proxy scam situation. The Barnum effect pertains to the acceptance of vague or neutral personality feedback that could apply to anyone as accurate description of one's personality (Forer, 1949). Manipulations include asking participants to rate the same feedback for how applicable it is to people in general (Johnson et al., 1985; Snyder & Larson, 1972) as well as including positively and negatively valenced feedback (Dana & Fouke, 1979; Furnham & Varian, 1988; Layne, 1978). In this study, the newly developed Susceptibility to Fraud Scale was distributed to participants along with Gudjonson (1984) Compliance scale and Sapp and Harrod (1993) Locus of Control scale. Participants were made to believe that, following the psychometric measures; they would be given their own personality feedback. Instead, all participants received the same, Barnum type personality feedback. The study included a series of analyses including looking into differences between high and low fraud susceptibility groups and non-victims and previous victims of fraud, as well as relationships between the subscales of the STFS and the agreement with Barnum type personality feedback.

6.4 Summary of the findings

The primary aim of this thesis was to construct a valid measure of susceptibility to fraud, in order to identify and evaluate the key components of fraud vulnerability. The initial framework was based on the findings of the interview study with victims of fraud and the review of different theoretical models and previous fraud literature. The interview study (Chapter 3) identified three stages of scam compliance from the perspective of the victim, which are: Precursors (e.g. situational factors), Commitment (e.g. factors that may influence scam compliance after the initial engagement) and Aftermath (e.g. processes that follow fraud victimisation). From this study, various themes emerged:

- Time constraints, such as urgency and lack of time to consider information
- Dissatisfaction with one's present circumstances

- Social influence
- Factors pertaining to the perpetrator, such as credibility, similarity and likeability, or limiting the availability of the offer
- Factors pertaining to the victim, such as excitement at the prospect of the offer, lack of scrutiny of information and social norms
- Psychological and financial consequences
- Forming avoidance strategies
- Seeking resolution and justice
- Loss of trust

The results demonstrated that there were many themes consistent with previous fraud literature, on techniques used by fraudsters, such as: limited availability or requiring an urgent response (Cialdini, 2001; Lea et al., 2009; Kramer & Carroll, 2009), and liking and similarity (Cialdini, 2011; Lea et al., 2009; Silvia, 2005). Additionally, individual characteristics that may influence compliance with fraudulent offers, such as: lack of self-control and impulsivity driven by excitement (Langenderfer & Shimp, 2011; Holtfreter et al., 2010; Lea et al., 2009; Modic & Lea, 2012, 2013), low motivation for information processing (Blythe et al., 2011; Lea et al., 2009; Kauffman et al., 1999) or social influence (Modic & Lea, 2013). Additionally, new themes emerged, such as formation of strategies for fraud avoidance, specifically those addressing vulnerability to fraud based on individual attributes and loss of trust and lack of empathy following fraud victimisation. Although previous research identified scam trajectories (Button et al., 2013; Whitty, 2013) and stages of the fraud process from the perspective of the perpetrator (Shadel & Pak, 2007), the interview study in this research programme was possibly the first to identify distinct stages fraud victims go through during the scam process, organising the factors that underlie them according to stage, and using the results for the construction of a psychometric measure. Although the final stage of the fraud process, the Aftermath, offered limited contribution to the construction of the scale (e.g. strategies constructed in order to compensate for vulnerability), it supported previous findings on the effects of fraud on victims (Button et al., 2013; Cross et al., 2014; Titus & Gover, 2001), reaffirming the need for better preventative measures.

The scale development study, Study 2 was based on the findings of the interview study with victims of fraud and the review of different theoretical models and previous fraud

literature (Lea et al., 2009; Modic & Lea, 2012, 2013). Findings from this study, regarding the subscales of the newly developed measure, supported theoretical models of Scamming Vulnerability (Langenderfer & Shimp, 2001) and Gullible Action (Greenspan, 2009). The Model of Scamming Vulnerability identified self-control as a moderator of scamming vulnerability under the visceral influence (Lanngenderfer & Shimp, 2001), which was confirmed by Impulsivity, a subscale of the STFS. Inability to control one's impulses and lack of self-control have also been mentioned as factors influencing scam compliance, as they compromise decision-making (Bayard et al., 2011; Holtfreter et al., 2010, 2015; Modic & Lea, 2012, 2013; Pratt et al., 2014). These findings also support a component of the Gullible Action Model (Greenspan, 2009), referring to state. More specifically, decisions made under the influence of strong emotions (hot cognition).

The model of Gullible Action also supported the findings referring to a subscale of the STFS concerned with delaying decisions, Decision Time, particularly that, when encountering misleading situations, delaying decisions may protect from gullible acts (Greenspan, 2009).

There were also topics, which arose from the fraud literature, such as liking and similarity and social norms (Cialdini, 2001; Lea et al., 2009; Whitty, 2013), such as not wanting to disappoint people, complying when pressured to make a decision, which ended up being part of the Compliance subscale. The final two subscales, Vigilance and Belief in Justice refer to literature on trust and vigilance in relation to predicting behaviour of others (Markóczy, 2003) and attitudes about justice and fraud victims, based on the findings of the interview study (Chapter 3), and fraud research (Cross, 2013; Lea et al., 2009). Comparing the newly developed STFS to an existing measure of Susceptibility to Persuasion (Modic & Lea, 2013), the first scale of its kind to measure concepts relating to scam compliance, demonstrated the concurrent validity of the STFS.

To test the utility of the STFS in Study 2, two email examples from a well-known technology company were used as test stimuli in order to examine participants' ability to correctly identify genuine email correspondence from a phishing email attempt. The results indicated that vigilant individuals and those that invest more time in making decisions were better at recognising phishing correspondence, whilst those with higher

scores on Compliance, Impulsivity and Belief in justice were less able to do so, indicating that the scale has a good predictive validity when it comes to phishing scams.

In Study 3, the Barnum effect was used as a proxy scam situation in order to evaluate the effectiveness of the STFS as an indicator of fraud susceptibility. In order to do this, high and low susceptibility groups were created. Participants in the high susceptibility group were less likely to see themselves as superior to others than those in low susceptibility group (i.e. high susceptibility individuals reported negative feedback as more true of them than those in low susceptibility group), driven primarily by Compliance and Impulsivity.

The study (Study 3) also found that previous fraud victims were more likely to assign higher scores to positive items than non-victims, but did not differ in their interpretation of the accuracy of negative or neutral feedback compared to non-victims. These results suggest that fraud victims may regard themselves as considering positive qualities to be a more accurate description of themselves than others, which may indicate fraud vulnerability in certain contexts. For example, overconfidence has been found to lead to judgment errors (Lea et al., 2009).

As it was expected that susceptible individuals would show the same pattern as victims of fraud, these conflicting results were unexpected, however, there may be an explanation for these results. Previous victimisation can in some cases be an indicator of future vulnerability, as some fraud victims have demonstrated an attraction to fraudulent offers (Lea et al., 2009), or are particularly vulnerable after being defrauded that it leads to future victimisation (Buchanan & Whitty, 2014; Whitty & Buchanan, 2016). However, it could be argued that not all victims are the same in that respect. For example, fraud affects a great number of people and can be extremely sophisticated in the way it is executed. Fraud can also be perpetrated without cooperation of the victim. Therefore, previous victimisation may not be a good indication of fraud vulnerability. This was supported by the findings, which indicated that participants who self-reported being defrauded previously were split between high and low susceptibility groups. Prior fraud victimisation may also result in greater vigilance. This was supported by the findings of the interview study, Study 1, with the majority of participants reporting that they have become aware of people's motives after the scam, which made them more diligent in checking information and questioning possible implications. The act of being scammed may therefore change someone's susceptibility to fraud in general.

Finally, fraud susceptibility may not always result in fraud victimisation. For example, one can be susceptible to fraud but also aware of this and able to compensate for it. This was also supported by the findings from Study 1. Therefore, previous fraud victimisation may not be a good indicator of general susceptibility to fraud.

6.4.1 Susceptibility to Fraud Scale

In the following sections, results of the Study 2 (Chapter 4) and Study 3 (Chapter 5) are discussed concurrently, in order to discuss the utility of the STFS subscales. Overview of the main research findings is shown in Table 6.1.

Table 6.1 Overview of research findings, with regards to subscales of the STFS

Subscale	**Study 2, Chapter 4**			**Study 3, Chapter 5**		
	Previous victim	Responded to scam offers in the past?	Able to recognise phishing attempt?	Previous victim	Overall acceptance of Barnum feedback	Acceptance of negative Barnum feedback
Compliance	(+)*		(-)			(+)
Impulsivity	(+)*	(+)	(-)	(+)*	(+)	(+)
Vigilance			(+)			
Decision time	(-)*	(-)	(+)			(-)
Belief in justice	(-)		(-)	(-)		

Notes.
(+) more likely to
(-) less likely to
* after controlling for age

6.4.1.1 STFS Compliance and Impulsivity as indicators of fraud vulnerability

Compliance, the subscale of the newly developed STFS scale, was found to be the best predictor of susceptibility to fraud. It was the factor with the strongest internal reliability (α=.87) and accounted for the largest proportion of the variance (16.41%) in STFS (Study 2, Chapter 4). Compliance predicted incorrect identification of phishing correspondence as genuine and also accounted for variations in previous fraud victimisation in Study 2.

In the Barnum Effect study (Study 3), compliant individuals assigned higher ratings for negative personality feedback items and lower ratings for positive personality feedback items than individuals who are less compliant. They were also less likely to see

themselves as superior to others, suggesting that individuals with higher scores on this factor may have a more negative view of self. Additionally, compliant individuals were also more likely to have an external Locus of Control, believe in chance and powerful others (Sapp & Harrod, 1993), which could indicate potential fraud vulnerability. For example, authority cues are frequently used in scam correspondence, therefore someone who believes in powerful others may be more influenced by communication purporting to be from credible authority sources. Additionally, there was a strong significant positive correlation between the STFS Compliance subscale and Gudjonson's (1989) Compliance scale, a measure of concurrent validity for Study 3.

The relationship between Compliance and a negative view of self supports the research by Gudjonson et al. (2002), whose findings indicated a positive relationship between compliance and low self-esteem as well as Fischer et al. (2013), who found a negative association between compliance and feelings of superiority. However, it is not clear if low self-esteem governs compliance or vice versa. Gudjonson et al. (2002) suggested that compliant individuals disagree with things they consciously decide to go along with. This awareness of one's weakness may lead to a negative view of the self. Alternatively, low self-esteem may be responsible for greater compliance in some situations. In the first study of this programme of research, some participants reported being vulnerable at the time they were defrauded and explicitly connected this vulnerability with their consequent compliance with a scam, despite having concerns at the time. One participant remembered feeling so desperate and eager to find a job, that even if she had found out about the company being fraudulent prior to paying a fee for a training pack, she may have gone ahead just in case it did work out. This may suggest that when people are at a low ebb in their lives and feel vulnerable, they are more likely to take risks. Participants that were defrauded when in difficult circumstances in their lives also seem to experience more psychological distress, which may contribute to reduced self-esteem, which in turn may make them more vulnerable to fraud.

The Compliance subscale is, therefore, a good indicator of susceptibility to fraud. It may also be a good indicator of one's self-esteem and vice versa. Compliance, as a construct, has not been extensively explored in relation to fraud, therefore, future studies may want to consider the relationship between self-esteem and compliance in relation to fraud vulnerability.

Lack of self-control has been found to be a factor implicated in vulnerability to fraudulent offers (Holtfreter et al., 2010, 2015; Langenderfer & Shimp, 2001; Lea et al., 2009; Modic & Lea, 2013) and this is especially pronounced when the victimisation happens online (Pratt et al., 2014). Additionally, Modic and Lea (2012) found premeditation (a facet of an impulsivity scale) to be a good predictor of scam compliance, with those who are not able to foresee the consequences more likely to engage with fraudulent offers. Impulsivity has also been found to affect decision-making process, with those that are more impulsive being more likely to take risks (Frederick, 2005) and purchase things from unknown vendors after receiving unsolicited email (Holtfreter et al., 2015).

The results of the Study 2 and 3 supported previous research on lack of self-control. Impulsivity was the second strongest predictor of susceptibility to fraud (explaining the 5.50% of the variance in STFS) with satisfactory internal reliability (α=.73). Scores on the Impulsivity scale also predicted the incorrect identification of phishing correspondence as genuine in Study 2 and was related to previous fraud victimisation in both, Study 2 and Study 3, after controlling for age, suggesting that more impulsive individuals may be less able to spot phishing correspondence, making them more likely to become fraud victims. Additionally, a positive relationship was found between Modic and Lea (2013) Self-Control subscale of StP scale, measuring lack of self-control, and STFS Impulsivity subscale, indicating that Impulsivity denotes lack of self-control with regards to fraudulent offers.

Additionally, in the Barnum Effect study (Study 3), impulsive individuals were more likely to assign higher ratings to negative personality feedback statements and were more likely to accept a greater number of statements irrespective of valence, suggesting they may be less likely to scrutinise information given to them. They were also more likely to believe in powerful others and chance, measured by Sapp and Harrod's (1993) Locus of Control measure.

Some authors have argued that, rather than indicating gullibility, greater acceptance of neutral and positive items refers to being rational, as most people tend to describe themselves using positive attributes (Layne, 1979). Therefore, greater acceptance of negative items may indicate that compliant and impulsive individuals are more likely to agree with people even when they are being told negative things about themselves.

Impulsivity and Compliance subscales, therefore, may be used as a reliable indicator of susceptibility to fraud.

6.4.1.2 Vigilance and Decision Time as moderators of fraud vulnerability

Vigilance and Decision time were subscales of the STFS, with slightly lower reliability than optimal (α=.65), however, both factors appeared to be good indicators of vulnerability to fraud. In Study 2, Vigilance and Decision Time scales predicted the correct identification of phishing correspondence. Additionally, negative relationships were found between these subscales and Impulsivity, as well as Compliance, indicating that more impulsive and compliant individuals are also less vigilant and spend less time making decisions. In Study 3, individuals that take time to make decisions accepted fewer negative personality statements as true descriptions of their personality and were less likely to believe in chance (Sapp & Harrod, 1993) and in Study 2 they were less likely to report responding to fraudulent offers based on hypothetical scam scenarios.

The Decision Time subscale explained 7.88% of the variance in STFS and represents a participant's preference for taking time to make decisions. According to Greenspan (2009), this attribute may protect from gullible action. This was also supported by the accounts of victims of fraud from Study 1 in this thesis. Rushing decisions and not considering information carefully, or not having the time to consider information, were frequently cited as a reason for fraud victimisation. These results can be explained in context of decision-making styles. For example, Scott and Bruce (1995) identified five decision- making styles; a rational style (search and evaluation of alternatives), an intuitive style (based on feelings), dependent style (based on advice), avoidant style (avoiding decisions) and spontaneous style (based on a desire for immediate decisions). In a series of studies exploring why consumers delay decisions, Greenleaf and Lehman (1995) found that some consumers delay decisions when they are too busy to devote the time to a decision due to other priorities, need the time to gather further information for comparison and want to obtain someone else's advice before purchasing. This suggests that preference for delaying decisions until there is time to carefully consider information may offer protection from fraud. Furthermore, making a rule to delay decisions may also offer protection from the effects of visceral influence. Scams often evoke visceral influence in order to bypass careful information processing (Cukier et al., 2007; Langenderfer & Shimp, 2001; Lowestein, 1996; Rusch, 1999), therefore delaying decisions would offer protection in situations that evoke visceral influence but would

also mean exerting self-control. However, factor analysis on an independent sample in Study 3 (Chapter 5) indicated that it may not be distinguished from Impulsivity. Therefore, the Decision Time subscale may be used as a general indication of preference for careful consideration, although it may benefit from further evaluation.

Little direct empirical evidence exists to link vigilance with fraud prevention or what "being vigilant" means in the context of fraud. Vigilance, a subscale of STFS was found to indicate an awareness of others' motives and preferences to check information given. Vigilance has been implicated in predicting the behaviour of others, with trusting individuals who were more vigilant being better at predicting others' behaviour than those found to be less vigilant (Markóczy, 2003). In Study 1, many participants reported that, since becoming a victim of a scam, they had grown more aware that others may not have honest motives, therefore they are now more careful to check small details and think about pros and cons. In Study 2, as well as correctly identifying phishing correspondence, vigilant individuals also reported receiving more fraudulent offers similar to the scenarios presented to them for consideration (Modic & Lea, 2013). This may indicate that generally, vigilance may be implicated in a greater awareness of fraudulent practices. Vigilant individuals also reported feeling more confident in their identification of email correspondence for both, genuine and phishing examples.

Vigilance has been identified as an important factor in the detection of insurance fraud, such as paying attention to irregularities in claimants' stories in order to detect deception (Morley, Ball, & Ormerod, 2006). Therefore, the STFS Vigilance subscale may provide a good general indicator of how aware one is of fraudulent practices in operation.

6.4.1.3 Belief in Justice

The reliability of some factors of the STFS fell below the recommended value widely quoted for indicating acceptable reliability (Cronbach's α, 0.7; DeVellis, 2012), with the Belief in Justice factor in particular suggesting a lack of internal consistency (α =.48). The questionnaire items that comprised this factor were retained in the item pool for couple of reasons. First was that in the interviews with victims of fraud (Chapter 3), where participants had reported the fraud to the authorities, they were often surprised to have their case ignored. They expressed disbelief that the authorities would turn their back on the crime that had been committed against them and they reported thinking,

prior to the victimisation, that they believed the "police would be all over it" once they reported the crime. This appeared to be a factor common to most victims. Second, was that some of the participants in the first study (Study1, Chapter 3) also reported that they were surprised they were defrauded as they considered themselves to be intelligent. They felt ashamed of being defrauded and some even openly commented that they felt embarrassed going to the police because they felt responsible for the crime. This finding was supported by Cross (2013, 2015), who found negative discourse around fraud victimisation, specifically that fraud victims are seen as greedy and therefore, they deserved what happened to them.

Holding an erroneous belief that fraud victimisation only happens to people who have certain attributes may be an indication of vulnerability, as would a belief that all crimes can be solved and prosecuted. In fact, research by Lea et al. (2009) also found that fraud victims believed the fraud, once reported, would be investigated and prosecuted and suggested that this may be down to the illusion of control. As the scale was intended to be a protective measure, a way to pinpoint areas of individual vulnerability to fraud, it was felt that being under the impression that all crimes would be investigated by the authorities or that only certain types of people are vulnerable to fraud, would make one less careful. As such, these beliefs may be an indication of vulnerability to fraud; therefore, this factor was put forward despite its low reliability.

The results of the reliability analysis for this factor appeared conflicting in that they indicated that removing any further items from the subscale would lower the reliability of the subscale, however, the inter-item correlations of the questionnaire items suggested that this factor may be measuring different concepts. Despite this, the factor remained as a stable component during each iteration of the factor analysis process in Study 2. Two items on the subscale; 'Only gullible people fall for scams' and 'I feel safe from becoming a victim of crime' had a correlation within the recommended range of .2 and .4 (Briggs & Cheek, 1986), as did the other two items 'Scammers and fraudsters normally will get caught in the end' and 'The Authorities, overall are effective at protecting us from crime'. However, all other correlations were below the recommended amount.[1]

[1] 'I feel safe from becoming a victim of crime' and 'The Authorities, overall are effective at protecting us 'Only gullible people fall for scams' and 'Scammers and fraudsters normally will get caught in the end'

The fact that participants who responded feeling safe from becoming a victim of a crime did not agree that the Authorities are effective at protecting them from crime as much as they agreed that only gullible people fall for scams points to the fact that there may be a latent variable underlying these items, such as an illusion of control, as mentioned by Lea et al. (2009). For example, feeling safe from becoming a victim of a crime because only gullible people fall for scams, could indicate an illusion of control over events that one has no control over, such as becoming a victim of a crime. This is probably more prominent with regards to fraud, as fraud is often seen as the victim's responsibility, even by victims themselves (Cross, 2013, 2015). However, increasing sophistication of some types of fraud means that no one is safe from fraud and in some cases, being defrauded does not require cooperation. Therefore, these items may seem to measure an illusion of control with regards to fraud victimisation, while the other two items refer to the effectiveness of the Authorities to punish perpetrators of fraud and as such, these items may be measuring people's belief in justice. Nevertheless, Belief in justice predicted previous fraud victmisation in both, Study 2 and Study 3. It was also implicated in the incorrect identification of the phishing email correspondence, with individuals that believe in justice more likely to identify phishing email as genuine, however the result was marginally significant (p=.046). Whilst it is clear the concepts evaluated by the scale are important, the factor may benefit from further development, potentially exploring and separating these two concepts.

6.5 The model of Fraud Susceptibility

In the present thesis, three unique studies were designed and executed in hope that they would pinpoint individual attributes that may be implicated in vulnerability to fraud. An interview study, which explored the scam process, in order to gain a new perspective and deeper understanding of the factors that influence compliance with fraudulent offers and two experimental studies, designed to test the newly developed measure of fraud susceptibility. This holistic approach allowed for better understanding of factors that increase or moderate vulnerability to fraudulent offers. As a result, the Model of Fraud Susceptibility was proposed (Figure 6.1).

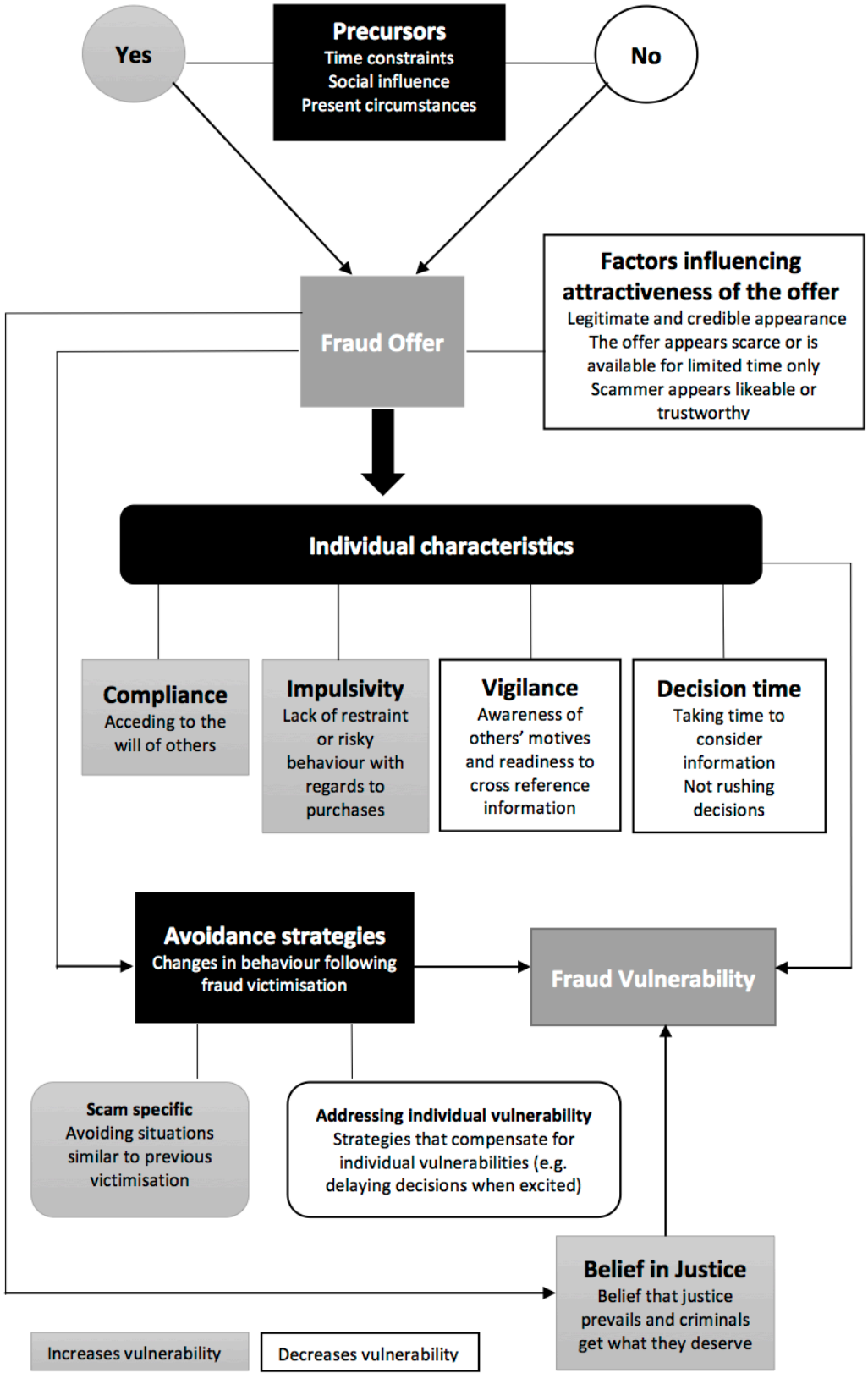


Figure 6.1 The Model of Fraud Susceptibility

The model outlines different influential components of vulnerability and takes into consideration all three studies in this programme of research.

When a fraudulent offer is received, or a product or a service is needed, there are certain factors that come into play, which may make the offer more attractive or simply make the engaging with the offer more likely. First, the precursors to the scam, or the circumstances the potential victim may find themselves in, such as having no time to carefully examine the offer or finding themselves in a situation that could be alleviated by the scam offer (e.g. needing a job). The offer will also appear more attractive if it looks like a genuine offer, is somehow limited (e.g. one day only deal) or appears scarce, and the source of the offer (e.g. a scammer or a website) appears trustworthy.

Once the potential victim deems the offer appropriate, they may comply with it immediately due to certain factors, either because they are more impulsive or because they are more likely to go along with things, even when they do not want to. However, they may decide that, although the offer looks legitimate, it may be worth checking facts before a decision is made or they may have a preference for taking time to think things over. Additionally, the potential victim may be aware that they are vulnerable to fraud and use strategies to avoid it. For example, although the offer looks attractive, the potential victim may be aware that, in the past, impulsive decisions led to undesirable outcomes, therefore they have learnt to delay their decisions, which may lead to a decreased emotional involvement and allow time for careful information processing.

The decision to go along with the offer may also be influenced by an individual's belief that scams only happen to certain people, inducing false confidence in the decision. The scam process may, therefore, be a very complex event, influenced by different components that contribute to scam compliance.

6.5 Original contribution and implications

The present research offers several contributions to fraud research. The newly developed measure of fraud susceptibility is the first scale constructed using a variety of analytical methods that measures facets of vulnerability to fraud. The scale items were specifically generated for this purpose, according to findings from an interview study

with victims of fraud, as well as previous fraud research and available models that may explain compliance with fraudulent offers. The present research offered empirical evidence to the Model of Scamming Vulnerability (Langenderfer & Shimp, 2001) and the Model of Gullible Action (Greenspan, 2009). It also indicated that certain beliefs may influence how careful someone is with regards to fraud as well as shown that compliance, as well as impulsivity, may be an influential factor in scam compliance. Additionally, the concept of vigilance was identified as a moderating factor of susceptibility to fraudulent offers as was a preference for careful deliberation prior to making decisions. Based on these findings, the Model of Fraud Susceptibility has been proposed.

The utility of the STFS was tested in two separate studies (Study 2 and Study 3), yielding results that have implications for future fraud research. The utility of the scale was also supported by evidence that the scale is highly related to similar measures, a Susceptibility to Persuasion scale (Modic & Lea, 2013) and Compliance Scale (Gudjonson, 1989). Additionally, the present research was the first to utlise the Barnum effect as a proxy scam measure.

The STFS and the Model of Fraud Susceptibility can be useful tools for fraud practitioners and be used to ascertain a level or areas of vulnerability. Additionally, the model may provide a basis for better preventative measures and advice to victims and potential victims.

6.5.1 Implications for fraud research

Throughout the present research, the focus has been on developing a measure that could be used as a fraud prevention tool, which resulted in a Susceptibility to Fraud Scale, measuring different areas of fraud susceptibility. As well as offering support to previous research on self-control and impulsivity (e.g. Modic & Lea, 2012, 2013), the present thesis identified other factors involved in susceptibility to fraud. Compliance with the wishes of others was found to indicate susceptibility to fraud as well as negative views of self. This supports previous research (Gudjonson, et al., 2002; Fischer et al., 2013) and may suggest a relationship between compliance and self-esteem, which warrants further research. Vigilance (Markóczy, 2003; Morley et al., 2006) and preference to delay making decisions in ambiguous situations (Greenspan, 2009; Greenleaf & Lehman, 1995) were also found to indicate susceptibility to fraud.

The concept of vigilant behaviour with regards to fraud is under researched. While some studies have attempted to look at trust in relation to scam compliance (Fischer et al., 2013; Workman, 2008), vigilance may be moderating the effects of trust and it is this vigilance that is crucial in determining if a trusting individual is naive or prudent (Markóczy, 2003). This may be crucial in fraudulent situations. The findings of the first and second study in this programme of research, indicated that vigilance and time allocated to decision making may be important in understanding why some people tend to recognise fraudulent offers when others do not. For example, Thunholm (2004) found a relationship between the intuitive and the spontaneous decision-making styles and suggested this may indicate that in some cases, such as where there is time pressure, the two styles may merge to create high speed intuitive style. This may be crucial in relation to fraudulent offers, especially those that create urgency. In the presence of urgency, when warnings signs are detected, one may choose to concentrate on the scammer or the scam offer instead, to justify the decision, as concentrating on risk would mean delaying the decision. In the first study of this programme of research, some participants reported having doubts about the situation but the time pressures made them concentrate on the positives instead (e.g. such as the attributes of the scammer or attaining the desired item). Thunholm (2004) further suggest that decision-style involves habit and as such, it may be possible to learn another habit. In context of fraud, this may mean delaying decisions until visceral influence has subsided or alternative information can be considered. These findings could therefore benefit from further research. Specifically, further studies should look into decision-making styles and fraud victimisation.

The results of the Barnum study, Study 3, and to some degree Study 1, identified that there may be fundamental differences in the attributes of individuals susceptible to fraud who progress to become victims and those that do not, which may have implications for future fraud research and prevention, and warrants further investigation.

6.5.2 Implications for fraud prevention practice

The present research found that reporting fraud leads to a loss of confidence and trust in authorities, which may result in a lack of fraud reporting, as well as cooperation with the authorities in the future. In addition, loss of trust may have long-term societal consequences, such as altering people's attitudes and leading to less empathy and trust

extended to others. Although it is impractical to follow up every case of fraud reported, an honest and more sympathetic way of addressing victims of fraud is needed. This could be achieved with more transparency about the likelihood of an investigation and prosecution, how complaints are processed and what the reporting data is likely to be used for. For example, if victims of fraud were treated more sympathetically and told that, although the investigation of their fraud case is unlikely, reporting fraud is vital for fraud prevention and policy making, as it identifies new fraud tactics and leads to improvements in fraud policing, they may be less likely to feel let down by the fraud justice system.

It is clear from previous research on security warnings (Egelman et al., 2008; Egelman & Peer, 2015; Frauenstein & Flowerday, 2016), that better fraud prevention is needed, one which goes beyond just listing and warning about the scams in operation. Most victims try to modify their behaviour following fraud victimisation, however, they do not always know how best to do this and may concentrate on scam delivery or content only, leaving them open to further victimisation. The Susceptibility to Fraud Scale may be used as an instrument for evaluating areas of vulnerability in order to determine what advice would be the most suitable. Additionally, the scale could be used in conjunction with the Model of Fraud Susceptibility, in order to raise awareness of individual attributes that contribute to or moderate vulnerability to fraud offers.

6.5.1 Implications for future research

Future research studies should concentrate on interviewing people that came close to being defrauded but realised it was a scam. Limited findings from Study 1 identified that some people are aware of aspects of their personality that make them more vulnerable to interpersonal influence in certain situations and have devised strategies that compensate for this. This is a fundamental step for fraud prevention. A deeper understanding of this self-awareness and coping strategies could improve advice given to victims and especially repeat victims of fraud.

Different types of scams rely on different motivational and cognitive factors. As such, the newly developed STFS may benefit from testing on different scam correspondence, in order to establish if it could be used as a valid general measure of vulnerability to fraud across different types of scams. This may also benefit future fraud prevention. For example, if it was established that compliance and impulsivity best predict certain types of scams and lack of vigilance other types of scams, people could be given advice

about scams that they may be more vulnerable to, according to their STFS scores.

Finally, future studies may also want to examine the role of self-esteem and fraud susceptibility, especially with regards to compliance and the acceptance of the negative feedback.

6.6 Considerations and limitations

Certain considerations and limitations have been noted with regards to studies reported in the present thesis.

6.6.1 Difficulty in measuring scam compliance

In order to ascertain if a measure indeed measures what it is supposed to measure, it has to demonstrate predictive validity. This is extremely difficult when measuring susceptibility to fraud. For example, in the studies conducted by Lea et al. (2009), a letter (sent in a plain envelope) with a questionnaire asking for people's opinions about a scam correspondence attached to the questionnaire and an explanation about the study, attracted fewer responses than a letter pretending to be a scam offer, that had a questionnaire attached after the offer is read. Therefore, measuring scam compliance is difficult without deception, as it may make people more cautious. The context, emotions, thoughts and possible consequences need to be 'real'.

Ideally, an experiment would measure individual characteristics connected to fraud susceptibility and compliance with the fraudulent offer at the same time; however, in order to do that, some type of scam needs to be simulated without the participants knowing about it. This methodology has proven to be extremely effective (e.g. Jagatic et al., 2007; Workman, 2008) but often poses serious ethical considerations. This includes causing psychological harm and distress to participants as fraud victimisation often elicits feelings of shame and embarrassment. However, the research by Jagatic et al. (2007) also unearthed some important methodological issues, too. For example, whilst most of the participants fell for a targeted phishing attack in their study, after the study, the participants only discussed the unethical nature of the research and expressed anger, with no one openly admitting to falling victim to a phishing attack used in the study. This may suggest that fraud victimisation, even in experimental contexts, tends to elicit secrecy. The study by Workman (2008), involved looking at fraud

vulnerability in a business organisation, in which employees agreed to monitoring beforehand. The study did not mention any negative consequences; however, it may be that employees felt they could not express anger at being used as unwitting participants in the fraud study due to the monitoring clause in their contract.

Therefore, in Study 2, examples of genuine and phishing email correspondence were used. Although, an incorrect identification of phishing correspondence may predict scam compliance in other contexts, it has to be emphasized that measuring fraud compliance by asking participants to decide if an email is real or fake may not be a true measure of scam compliance. In a real-life situation, such an email might evoke strong emotional reaction, which is likely to influence compliance. However, given the fact that the STFS predicted those who incorrectly identified phishing correspondence as genuine, despite the fact that participants were able to rationally think about their choices, unaffected by factors that influence errors in judgments, it may also be a good predictor of vulnerability to phishing correspondence in real-life contexts. Additionally, this method of testing scam compliance, although not perfect, may be a good way of measuring scam compliance in a way that is not harmful to participants.

The Barnum effect may not have been an appropriate proxy scam measure of general scam compliance. The results of the Barnum study, Study 3, did not follow the usual pattern as predicted (e.g. acceptance of neutral and positive items as more true on oneself than negative items). However, as this is the first time the Barnum effect has been used in the context of fraud, using a newly developed measure, it is difficult to say how applicable it is as a proxy scam situation, without further testing.

6.6.2 Sampling considerations

There are certain sampling considerations worth mentioning. In Study 1, one of the participants came close to being defrauded but realized in time. Furthermore, the same participant reported having rules and strategies in place to get out of situations where he may be put under pressure to comply, due to the fact that he finds it difficult to say no. It would have been advantageous to explore additional accounts of near victims, especially if they are aware of areas of their personality that may be vulnerable to persuasion or fraudulent communication and to explore the decisive factors that caused them to withdraw from the scam. However, it proved difficult to recruit participants that fit these criteria. The study found that victims of fraud often felt they were ignored

by the authorities, and were therefore willing to tell someone their side of the story, but this may not be of importance to those that are used to avoiding fraudulent offers that come their way. There is a possibility that, with more participants fitting these criteria, different conclusions would have been reached.

Studies 2 and 3 in the present thesis relied heavily on student participants. Even though the studies attracted a great number of participants of all ages, about a third of the sample in each of these studies comprised of participants aged between 18 and 22 years of age. Although this is not unusual in psychology research, it often poses certain limitations. Studies have found that students differ in characteristics from general population and especially from older adults (Foot & Sanford, 2004; Sears, 1989). For example, Sears (1989) argues that students have less formulated sense-of-self and comply with authority more readily, and that age is an influential factor in people's attitudes.

Present research found that younger participants were more susceptible to fraud, were more likely to be more compliant and impulsive, however, they were less likely to report previous fraud victimisation, which may be due to the amount of exposure to fraudulent offers. Modic and Lea (2012) noted similar findings. Therefore, it may be sensible not to rely on student participants in fraud research.

6.6.3 Other limitations

In Study 2 and Study 3, participants were asked if they have previously been defrauded. However, they were not asked to explain the nature of the fraud experience, such as what type of fraud it was or how long the communication, if any, with the scammer was. In hindsight, this question should have been asked, as this information may have provided an insight into why previous fraud victims responded differently to the Barnum type feedback than individuals susceptible to fraud, as not all frauds require the same amount of cooperation from the victim. Additionally, while some frauds are obvious, there are others, which are extremely sophisticated. Therefore, knowing this information would have been helpful in exploring fraud susceptibility with regards to previous fraud victims.

6.7 Conclusion

The idea that 'one cannot cheat an honest man' is still prevalent today, as the discourse around fraud victimisation revolves around greed and blame. Society, perpetrators and the victims themselves assign the blame and the responsibility for the fraud victimisation to the victim. Fraud causes great psychological harm. The costs of fraud victimisation are not only monetary but also societal. Fraud erodes trust in the fellow man as well as trust in the society and the effectiveness of the authorities to provide a safe, law-abiding environment for its citizens. Therefore, fraud victimisation should not be dismissed as a lesser crime as it so often is. Although the costs of fraud investigations and prosecutions are high and investigating some types of online fraud is an impossible task due to the cross-border element, there is plenty that can be done to improve fraud prevention measures. Taking an individual approach means that, rather than overwhelming victims and potential victims with information that is not applicable to them, victims could be given more effective advice on how to compensate for their vulnerabilities with regards to fraud.

The present research used a variety of methods in order to construct a measure of fraud susceptibility. Through the narratives of fraud victims in Study 1 (Chapter 3), processes that underlie fraud victimisation were identified and successfully used, along with previous fraud research and theoretical models, to develop Susceptibility to Fraud Scale in Study 2 (Chapter 4). The newly developed measure is comprised of five subscales: Compliance, Impulsivity, Vigilance, Decision Time and Belief in Justice.

The STFS was able to discriminate between previous fraud victims and non-victims in Study 2, with Compliance, Impulsivity and Belief in Justice, associated with increased fraud vulnerability. It was also able to discriminate participants who could correctly identify phishing email correspondence and those who could not. In addition, the present research provides an important contribution to understanding factors that underlie vulnerability to fraudulent offers, especially with regards to protective factors, such as increased vigilance and a preference to delay decisions and consider the available information.

The utility of the STFS was also tested on a proxy scam situation, utilising the Barnum effect paradigm in Study 3 (Chapter 5), the first study to use the Barnum effect as a measure of susceptibility to fraud. A connection between high susceptibility to fraud

and the acceptance of the negatively valenced feedback was found, with individuals in the high fraud susceptibility group more likely to view others as superior to them than those in the low fraud susceptibility group, driven mostly by Compliance and Impulsivity. Additionally, impulsive individuals were more likely to agree with any statements.

The findings in this thesis indicated that individual characteristics may be important indicators of vulnerability to fraud. The proposed Model of Fraud Susceptibility is based on evidence across all three studies in this thesis, and as such, it provides the basis for more individual and victim orientated approach to fraud prevention.

References

ActionFraud. Retrieved from: http://www.actionfraud.police.uk/what-is-fraud (Accessed 20th August, 2017)

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of occupational and organizational psychology*, *63*(1), 1-18.

Ariely, D., & Loewenstein, G. (2006). The heat of the moment: The effect of sexual arousal on sexual decision making. *Journal of Behavioral Decision Making*, *19*(2), 87-98.

Bayard, S., Raffard, S., & Gely-Nargeot, M. C. (2011). Do facets of self-reported impulsivity predict decision-making under ambiguity and risk? Evidence from a community sample. *Psychiatry Research*, *190*(2), 322-326.

Beals, M., DeLiema, M., & Deevy, M. (2015). Framework for a taxonomy of fraud. *Washington DC: Stanford Longevity Center/FINRA Financial Investor Education Foundation/Fraud Research Center*.
Available online at: http://162.144.124.243/~longevl0/wp-content/uploads/2016/03/Full-Taxonomy-report.pdf (Accessed 10th July 2018)

Beins, B. C. (1993). Using the Barnum effect to teach about ethics and deception in research. *Teaching of Psychology*, *20*(1), 33-35.

Bentler, P. M., & Kano, Y. (1990). On the equivalence of factors and components. *Multivariate Behavioral Research, 25*(1), 67-74.

Benton, A. A., Kelley, H. H., & Liebling, B. (1972). Effects of extremity of offers and concession rate on the outcomes of bargaining. *Journal of Personality and Social Psychology*, *24*(1), 73.

Blais, A. R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, 1(1), 33–47.

Blythe, M., Petrie, H., & Clark, J. A. (2011, May). F for fake: four studies on how we fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*(pp. 3469-3478). ACM.

Braun, V. & Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), pp.77-101.

Briggs, S. R., & Cheek, J. M. (1986). The role of factor analysis in the development and evaluation of personality scales. *Journal of personality*, *54*(1), 106-148.

Bruner, J. S. (2003). *Making stories: Law, literature, life*. Harvard University Press.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the Association for Information Science and Technology*, *58*(2), 157-165.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261-283.

Burman, E. (1994). Interviewing. *Qualitative methods in psychology: A research guide*, 49-71. Maidenhead, Berkshire: Open University Press.

Button, M., Lewis, C., & Tapley, J. (2009a). Fraud typologies and the victims of fraud: literature review. Available online at: https://researchportal.port.ac.uk/portal/files/1926122/NFA_report3_16.12.09.pdf (Accessed 17th August 2017)

Button, M., Lewis, C., & Tapley, J. (2009b). Support for the victims of fraud: An assessment of the current infrastructure in England and Wales. Available from: https://researchportal.port.ac.uk/portal/files/1926164/support-for-victims-of-fraud.pdf (Accessed 17th August 2017)

Button, M., Gee, J., Lewis, C. & Tapley, J., (2010). The human cost of fraud: A vox populi. *Centre for Counter Fraud Studies & MacIntyre Hudson. Portsmouth: University of Portsmouth*. Available online at:

http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/cost-of-fraud.pdf (Accessed 17th August 2017)

Button, M., Lewis, C., Shepherd, D., Brooks, G., & Wakefield, A. (2012). Fraud and punishment: enhancing deterrence through more effective sanctions. *Centre for Counter Fraud Studies, Portsmouth: University of Portsmouth*. Available online at: https://www.researchgate.net/profile/Mark_Button3/publication/299377462_Fraud_and_Punishment_Enhancing_Deterrence_Through_More_Effective_Sanctions/links/56f2afa508aeb55674eb50ea.pdf (Accessed 20th August, 2017)

Button, M., Tapley, J., & Lewis, C. (2013). The 'fraud justice network'and the infra-structure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice*, *13*(1), 37-61.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36-54.

Button, M., Blackbourn, D., & Tunley, M. (2014). 'The Not So Thin Blue Line After All?' Investigative Resources Dedicated to Fighting Fraud/Economic Crime in the United Kingdom. *Policing: A Journal of Policy and Practice*, *9*(2), 129-142.

Button, M., McNaughton Nicholls, C., Kerr, J., & Owen, R. (2015). Online fraud victims in England and Wales: victims' views on sentencing and the opportunity for restorative justice?. *The Howard Journal of Crime and Justice*, *54*(2), 193-211.

Button, M., Gee, J. & Mothershaw, N. (2016). Annual Fraud Indicator. Available online at: http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf (Accessed on 14th December 2017)

Button, M., Gee, J. & Mothershaw, N. (2017). Annual Fraud Indicator. Available online at: https://www.croweclarkwhitehill.co.uk/wp-content/uploads/sites/2/2017/11/Annual-fraud-indicator-2017.pdf (Accessed on 14th December 2017)

Cacciottolo, M. and Rees, N. (2017). Online dating fraud victim numbers at record high. *BBC News*. Available online at: http://www.bbc.com/news/uk-38678089 (Accessed 31st October 2017)

Cacioppo, J.T & Petty, R.E. (1982). The need for cognition. *Journal of personality and social psychology*, *42*(1), 116-131.

Cacioppo, J. T., Petty, R. E., & Feng Kao, C. (1984). The efficient assessment of need for cognition. *Journal of personality assessment*, *48*(3), 306-307.

Cacioppo, J. T., Petty, R. E., Kao, C. F., & Rodriguez, R. (1986). Central and peripheral routes to persuasion: An individual difference perspective. *Journal of personality and social psychology*, *51*(5), 1032.

Callahan, C. M., Unverzagt, F. W., Hui, S. L., Perkins, A. J., & Hendrie, H. C. (2002). Six-item screener to identify cognitive impairment among potential subjects for clinical research. *Medical care*, *40*(9), 771-781.

Chang, J. H., & Lee, K. H. (2010). Voice phishing detection technique based on minimum classification error method incorporating codec parameters. *IET signal processing*, *4*(5), 502-509.

Cialdini, R. B. (2001). Science and practice. Allyn & Bacon

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol.*, *55*, 591-621.

CIFAS (2014). Fraudscape. UK Fraud Trends.
Available online at:
https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External%20-%20Fraudscape%20main%20report%20for%20website.pdf (Accessed, 15th October 2017)

Citizen advice (2017), Changing the story on scams. Available online at: https://www.citizensadvice.org.uk/changing-the-story-on-scams/ (Accessed 5th August, 2017)

Collins, R. W., Dmitruk, V. M., & Ranney, J. T. (1977). Personal validation: Some empirical and ethical considerations. *Journal of Consulting and Clinical Psychology*, *45*(1), 70.

Collodi, C. (2011). Pinocchio. London, England. Penguin Books. [First published in 1882]

Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical assessment, research and evaluation, 10*(7), 1-9.

Cross, C., 2013. "Nobody's holding a gun to your head". Examining current discourses surrounding victims of online fraud. In *Crime, justice and social democracy: Proceedings of the 2nd International Conference* (Vol. 1, pp. 25-32). Crime and Justice Research Centre, Queensland University of Technology.

Cross, C., (2015). No laughing matter. Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), pp.187-204.

Cross, C. (2016). Policing online fraud in Australia: The emergence of a victim-oriented approach. In *Crime, Justice and Social Democracy: Proceedings of the 3rd International Conference 2015* (Vol. 1, pp. 1-8). Crime and Justice Research Centre, QUT.

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, *518*, 1-14.

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends & Issues in Crime and Criminal Justice*, *474*.

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007, January). Genre, narrative and the" Nigerian Letter" in electronic mail. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 70-70). IEEE.

Cuperman, R., Robinson, R. L., & Ickes, W. (2014). On the malleability of self-image in individuals with a weak sense of self. *Self and Identity*, *13*(1), 1-23

Dalbert, C. (1998). Belief in a just world, well-being, and coping with an unjust fate. In Montada, L., and Lerner, M. J. (eds.), *Responses to victimization and belief in a just world*. Plenum, New York, pp. 87-105.

Dalbert, C. (1999). The world is more just for me than generally: About the personal belief in a just world scale's validity. *Social Justice Research*, *12*(2), 79-98.

Dana, R. H., & Fouke, H. P. (1979). Barnum statements in reports of psychological assessment. *Psychological Reports*, *44*(3_suppl), 1215-1221.

Davies, M. F. (1997). Positive test strategies and confirmatory retrieval processes in the evaluation of personality feedback. *Journal of personality and social psychology*, *73*(3), 574.

DeVellis, R. F. (2012). *Scale development: Theory and applications* (Vol. 26). Sage publications.

Doig, A., Johnson, S., & Levi, M. (2001). New public management, old populism and the policing of fraud. *Public Policy and Administration*, *16*(1), 91-113.

Duffield, G. M., & Grabosky, P. N. (2001). *The psychology of fraud* (Vol. 199). Canberra: Australian Institute of Criminology.

Dutton, W. H., & Shepherd, A. J. (2004). *Confidence and risk on the Internet*. Foresight Directorate.
Available online at:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.492.9219&rep=rep1&type=pdf (Accessed 31st October 2017)

Egelman, S., Cranor, L. F., & Hong, J. (2008, April). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074). ACM.

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873-2882). ACM.

Evans, A. M., & Revelle, W. (2008). Survey and behavioral measurements of interpersonal trust. *Journal of Research in Personality*, *42*(6), 1585-1593.

Experian (2010). Insight Report.
Available online at: http://www.experian.co.uk/assets/insight-reports/brochures/The-Insight-Report-Victims-of-fraud-survey-March-2010.pdf
(Accessed 19th December 2017)

Field, A., & Hole, G. (2003). *How to design and report experiments*. Sage Publications.

Fischer, P., Lea, S. E., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*, *43*(10), 2060-2072.

Fischer, P., Jonas, E., Frey, D., & Kastenmüller, A. (2008). Selective exposure and decision framing: The impact of gain and loss framing on confirmatory information search after decisions. *Journal of Experimental Social Psychology*, *44*(2), 312-320.

Fletcher, C., Taylor, P., & Glanfield, K. (1996). Acceptance of personality questionnaire feedback: The role of individual difference variables and source of interpretation. *Personality and Individual Differences*, *20*(2), 151-156.

Frauenstein, E. D., & Flowerday, S. V. (2016, August). Social network phishing: Becoming habituated to clicks and ignorant to threats?. In *Information Security for South Africa (ISSA), 2016* (pp. 98-105). IEEE.

Frederick, S. (2005). Cognitive reflection and decision making. *The Journal of Economic Perspectives*, *19*(4), 25-42.

Forer, B. R. (1949). The fallacy of personal validation: a classroom demonstration of gullibility. *The Journal of Abnormal and Social Psychology*, *44*(1), 118.

Foot, H. and Sanford, A., The Use and Abuse of Student Participant, *The Psychologist,* 2004, Vol 17, No. 5.

Foozy, C. F. M., Ahmad, R., & Abdollah, M. F. (2013). Phishing detection taxonomy for mobile device. *International Journal of Computer Science Issues (IJCSI)*, *10*(1), 338-344.

Ford, J. K., MacCallum, R. C., & Tait, M. (1986). The application of exploratory factor analysis in applied psychology: A critical review and analysis. *Personnel psychology, 39*(2), 291-314.

Furnell, S., & Thomson, K. L. (2009). Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, *2009*(11), 7-11.

Furnham, A. (1989). Personality and the acceptance of diagnostic feedback. *Personality and Individual Differences*, *10*(11), 1121-1133.

Furnham, A., & Varian, C. (1988). Predicting and accepting personality test scores. *Personality and Individual Differences*, *9*(4), 735-748.

Gendall, P. (2005). Can you judge a questionnaire by its cover? The effect of questionnaire cover design on mail survey response. *International journal of public opinion research*, *17*(3), 346-361.

Glickman, H., 2005. The Nigerian "419" advance fee scams: prank or peril?. *Canadian Journal of African Studies/La Revue canadienne des études africaines*, *39*(3), pp.460-489.

Goffman, E., 1952. On cooling the mark out: Some aspects of adaptation to failure. *Psychiatry*, *15*(4), pp.451-463.

Grabosky, P. N., & Duffield, G. M. (2001). *Red flags of fraud*. Australian Institute of Criminology.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *30*(4), 395-410.

Greenleaf, E. A., & Lehmann, D. R. (1995). Reasons for substantial delay in consumer decision making. *Journal of Consumer Research*, *22*(2), 186-199.

Greenspan, S. (2008). Foolish Action in Adults with Intellectual Disabilities: The Forgotten Problem of Risk-Unawareness. *International review of research in mental retardation*, *36*, 147-194.

Greenspan, S. (2009). *Annals of Gullibility: Why We Get Duped and How to Avoid It: Why We Get Duped and How to Avoid It*. Westport, CT. Praeger Publishers.

Greenspan, S., Switzky, H. N., & Woods, G. W. (2011). Intelligence involves risk-awareness and intellectual disability involves risk-unawareness: Implications of a theory of common sense. *Journal of Intellectual and Developmental Disability*, *36*(4), 246-257.

Grierson, J. (2016). Met chief suggests banks should not refund online fraud victims. The Guardian. Available online at: https://www.theguardian.com/uk-news/2016/mar/24/dont-refund-online-victims-met-chief-tells-banks (Accessed 17th November, 2017)

Griffiths, M. A., & Harmon, T. R. (2011). Aging consumer vulnerabilities influencing factors of acquiescence to informed consent. *Journal of Consumer Affairs*, *45*(3), 445-466.

Gudjonsson, G. H. (1987). A parallel form of the Gudjonsson Suggestibility Scale. *British Journal of Clinical Psychology, 26*(3), 215-221.

Gudjonsson, G. H. (1989). Compliance in an interrogative situation: A new scale. *Personality and Individual Differences*, *10*(5), 535-540.

Gudjonsson, G. H., Sigurdsson, J. F., Brynjólfsdóttir, B., & Hreinsdóttir, H. (2002). The relationship of compliance with anxiety, self-esteem, paranoid thinking and anger. *Psychology, Crime and Law*, *8*(2), 145-153.

Haddock, G., Maio, G. R., Arnold, K., & Huskinson, T. (2008). Should persuasion be affective or cognitive? The moderating effects of need for affect and need for cognition. *Personality and Social Psychology Bulletin*, *34*(6), 769-778.

Halperin, K., Snyder, C. R., Shenkel, R. J., & Houston, B. K. (1976). Effects of source status and message favorability on acceptance of personality feedback. *Journal of Applied Psychology*, *61*(1), 85.

Harries, P.A., Davies M.L., Gilhooly, K.J., Gilhooly, M.L.M., & Cairns, D. (2013). Detection and prevention of financial abuse against elders. *Journal of Financial Crime*, *21*(1), 84-99.

Herley, C. (2012). Why do Nigerian Scammers say they are from Nigeria? *Microsof research,* In *WEIS*.

Hiss, F. (2015). Fraud and Fairy Tales: Storytelling and Linguistic Indexicals in Scam E-mails. *International Journal of Literary Linguistics*, *4*(1).

Holm, S. (1979). A simple sequentially rejective multiple test procedure. *Scandinavian journal of statistics*, 65-70.

Holtfreter, K., Reisig, M.D. and Pratt, T.C., 2008. Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), pp.189-220.

Holtfreter, K., Reisig, M. D., Leeper Piquero, N., & Piquero, A. R. (2010). *Criminal Justice and Behavior*, *37*(2), 188-203.

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, *21*(7), 681-698.

Hutchings, A., & Hayes, H. (2008). Routine activity theory and phishing victimisation: Who gets caught in the net. *Current Issues Crim. Just.*, *20*, 433.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of elder abuse & neglect*, *26*(2), 107-122.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A practical analysis of smartphone security. *Human Interface and the Management of Information. Interacting with Information*, 311-320.

Johnson, J. T., Cain, L. M., Falke, T. L., Hayman, J., & Perillo, E. (1985). The" Barnum effect" revisited: Cognitive and motivational factors in the acceptance of personality descriptions. *Journal of Personality and Social Psychology*, *49*(5), 1378.

Kaufman, D. Q., Stasson, M. F., & Hart, J. W. (1999). Are the tabloids always wrong or is that just what we think? Need for cognition and perceptions of articles in print media. *Journal of Applied Social Psychology*, *29*(9), 1984-2000.

Kerr J, Owen R, McNaughton Nicholls C & Button M. (2013). Research on sentencing online fraud offences. London: Sentencing Council. Available online at: https://www.sentencingcouncil.org.uk/wp-content/uploads/Research_on_sentencing_online_fraud_offences.pdf (Accessed 18th December 2017).

Kerley, K. R., & Copes, H. (2002). Personal fraud victims and their official responses to victimization. *Journal of Police and Criminal Psychology*, *17*(1), 19-35.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, *44*(2), 544-564.

King, N., & Horrocks, C. (2010). *Interviews in qualitative research*. London. Sage Publications.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual review of psychology*, *50*(1), 569-598.

Kramer, T., & Carroll, R. (2009). The effect of incidental out-of-stock options on preferences. *Marketing Letters*, *20*(2), 197-208.

Kvale, S., & Brinkmann, S. (2009). *Learning the craft of qualitative research interviewing*. Thousand Oaks. CA. Sage Publications.

Langenderfer, J. and Shimp, T.A., 2001. Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), pp.763-783.

Layne, C. (1978). Relationship between the "Barnum Effect" and personality inventory responses. *Journal of clinical psychology*, *34*(1), 94-97.

Layne, C. (1979). The Barnum effect: Rationality versus gullibility? *Journal of Consulting and Clinical Psychology*, *47*(1), 219.

Lea, S., Fischer, P., & Evans, K. (2009). The psychology of scams: Provoking and committing errors of judgement. *Report for the Office of Fair Trading*. Available online from: *https://ore.exeter.ac.uk/repository/bitstream/handle/10871/20958/OfficeOfFairTrading%202009.pdf?sequence=1&isAllowed=y* (Accessed 20th August, 2017)

Legard, R., Keegan, J. and Ward, K., 2003. In-depth interviews. *Qualitative research practice: A guide for social science students and researchers*, pp.138-169.

Lerner, M. J. (1965). Evaluation of performance as a function of performer's reward and attractiveness. *Journal of Personality and Social Psychology*, *1*(4), 355.

Lerner, M. J., & Miller, D. T. (1978). Just world research and the attribution process: Looking back and ahead. *Psychological bulletin*, *85*(5), 1030.

Löckenhoff, C. E., & Carstensen, L. L. (2007). Aging, emotion, and health-related decision strategies: motivational manipulations can reduce age differences. *Psychology and aging*, *22*(1), 134.

Loewenstein, G. (1996). Out of control: Visceral influences on behavior. *Organizational behavior and human decision processes*, *65*(3), 272-292.

Loveday, B. (2017). Still plodding along? The police response to the changing profile of crime in England and Wales. *International Journal of Police Science & Management*, 1461355717699634.

Luhmann, N., 2000. Familiarity, confidence, trust: Problems and alternatives. *Trust: Making and breaking cooperative relations*, *6*, pp.94-107.

Macdonald, D. J., & Standing, L. G. (2002). Does self-serving bias cancel the Barnum Effect?. *Social Behavior and Personality: an international journal*, *30*(6), 625-630.

Maggi, F. (2010, June). Are the con artists back? a preliminary analysis of modern phone frauds. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on* (pp. 824-831). IEEE.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

Markóczy, L. (2003, July). Trust but verify: Distinguishing distrust from vigilance. In *Academy of Management Conference*.

Martin, N. (2009). Consumer scams and the elderly: Preserving independence through shifting default rules. *Elder LJ*, *17*, 1.

Massi Lindsey, L. L. (2005). Anticipated guilt as behavioral motivation: An examination of appeals to help unknown others through bone marrow donation. *Human Communication Research*, *31*(4), 453-481.

Mason, K.A. and Benson, M.L., 1996. The effect of social support on fraud victims' reporting behavior: A research note. *Justice Quarterly*, *13*(3), pp.511-524.

Mason, O. J., & Budge, K. (2011). Schizotypy, self-referential thinking and the Barnum effect. *Journal of behavior therapy and experimental psychiatry*, *42*(2), 145-148.

Misztal, B., 2013. *Trust in modern societies: The search for the bases of social order*. John Wiley & Sons.

Mitchell, R. W. (1996). The psychology of human deception. *Social Research*, 819-861.

Modic, D., & Lea, S. E. (2012). How Neurotic are Scam Victims, Really? The Big Five and Internet Scams. Available online at SSRN: https://ssrn.com/abstract=2448130 (Accessed 29th November, 2017)

Modic, D., & Lea, S. E. (2013). Scam Compliance and the Psychology of Persuasion (June 21, 2013). Available online at SSRN: https://ssrn.com/abstract=2364464 (Accessed 29th November, 2017)

Modic, D., & Anderson, R. J. (2014a). We will make you like our research: The development of a susceptibility-to-persuasion scale. Available online at: https://papers.ssrn.com/soL3/papers.cfm?abstract_id=2446971 (Accessed 25th October, 2017)

Modic, D., & Anderson, R. (2014b). Reading this may harm your computer: The psychology of malware warnings. *Computers in Human Behavior*, *41*, 71-79.

Mohapatra, S. (2012). Stateless babies & adoption scams: a bioethical analysis of international commercial surrogacy. *Berkeley J. Int'l L.*, *30*, 412.

Molloy, M (2016). Astronaut stranded in space email scam sweeps the internet. *The Telegraph*. Available online at: http://www.telegraph.co.uk/news/newstopics/howaboutthat/12160621/Nigerian-astronaut-lost-in-space-email-419-scam-sweeps-the-internet.html (Accessed 29th September, 2017)

Morley, N. J., Ball, L. J., & Ormerod, T. C. (2006). How the detection of insurance fraud succeeds and fails. *Psychology, Crime & Law*, *12*(2), 163-180.

Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014, July). Towards an ontological model defining the social engineering domain. In *IFIP International Conference on Human Choice and Computers* (pp. 266-279). Springer, Berlin, Heidelberg.

Muscat, G., Graycar, A., & James, M. P. (2002). *Older people and consumer fraud*. Canberra: Australian Institute of Criminology.

National Fraud Authority (2010). Annual Fraud Indicator. Available online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118536/afi-2010.pdf (Accessed on 14th December 2017)

National Fraud Authority (2011). Annual Fraud Indicator. Available online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118532/annual-fraud-indicator-2011.pdf (Accessed on 14th December 2017)

National Fraud Authority (2012). Annual Fraud Indicator. Available online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf (Accessed on 14th December 2017)

National Fraud Authority (2013). Annual Fraud Indicator. Available online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf (Accessed on 14th December 2017)

National Trading Standards (2016). Friends Against Scams. Silence of the Scams: Progress, Practice and Prevention Conference, Brunel University London

Nikiforova, B., & W. Gregory, D. (2013). Globalization of trust and internet confidence emails. *Journal of Financial Crime*, *20*(4), 393-405.

Nunnally, J. C. (1967). *Psychometric theory*. New York. McGraw-Hill.

Nunnally, J. C. (1978). *Psychometric theory*. New York. McGraw-Hill.

O'Dell, J. W. (1972). PT Barnum explores the computer. *Journal of Consulting and Clinical Psychology*, *38*(2), 270.

Office of National Statistics (2016). Overview of Fraud Statistics.
Available online at:
https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016
(Accessed on 14th December 2017)

Olivier, S., Burls, T., Fenge, L. A., & Brown, K. (2015). "Winning and losing": vulnerability to mass marketing fraud. *The Journal of Adult Protection*, *17*(6), 360-370.

Orman, H. (2013). The compleat story of phish. *IEEE Internet Computing*, *17*(1), 87-91.

Orpen, C., & Jamotte, A. (1975). The acceptance of generalized personality interpretations. *The Journal of social psychology*, *96*(1), 147-148.

Pallant, J. (2013). *SPSS survival manual*. McGraw-Hill Education (UK).
Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, *2012*(1), 8-11.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*. Available from*: http://www.swdsi.org/swdsi2009/Papers/9J05.pdf* (Accessed 29th September, 2017)

Pascoe, T., Owen, K., Keats, G., & Gill, M. (2006). Identity fraud: What about the victim. *London: CIFAS*. Available online at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Identity%20Fraud%20%20What%20About%20the%20Victim%20Research%20Findings.pdf (Accessed 29th February, 2018)

Petty, R. E., & Cacioppo, J. T. (1986). Communication and Persuasion. Central and peripheral routes to attitude change. Springer, New York, NY.

Petty, R. E., Cacioppo, J. T., Kao, C. F., & Rodrigues, R. (1986). Central and peripheral routes to persuasion: An individual difference perspective. *Journal of Personality and Social Psychology*, *51*(5), 1032-1043.

Piper-Terry, M. L., & Downey, J. L. (1998). Sex, gullibility, and the Barnum effect. *Psychological Reports*, *82*(2), 571-576.

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self‐control and victimization: A meta‐analysis. *Criminology*, *52*(1), 87-116.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Reed, A. E., & Carstensen, L. L. (2012). The theory behind the age-related positivity effect. *Frontiers in psychology*, *3*, 339.

Rege, A. (2009). What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, *3*(2), 494.

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime*, *20*(3), 324-337.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior*, *36*(4), 369-384.

Robson, C. (2011). *Real world research*. Chichester. West Sussex. John Wiley and Sons.

Rosen, G. M. (1975). Effects of source prestige on subjects' acceptance of the Barnum effect: Psychologist versus astrologer. *Journal of Consulting and Clinical Psychology*, *43*(1), 95.

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American psychologist*, *35*(1), 1.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, *23*(3), 393-404.

Rusch, J. J. (1999, June). The "social engineering" of internet fraud. In *Internet Society Annual Conference*. Available online at: http://taupe.free.fr/book/psycho/social%20engineering/TheSocial%20Engineering%20of%20Internet%20Fraud.pdf (Accessed 15th December, 2017)

Saunders, K. M., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology*, *13*(2), 183-192.

Sapp, S. G., & Harrod, W. J. (1993). Reliability and validity of a brief version of Levenson's locus of control scale. *Psychological Reports*, *72*(2), 539-550.

Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and applied social psychology*, *36*(3), 272-279.

Schonemann, P. H. (1990). Facts, fictions, and common sense about factors and components. *Multivariate Behavioral Research, 25*(1), 47-51.

Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*, *16*(3), 633-654.

Schreck, C. J., Stewart, E. A., & Fisher, B. S. (2006). Self-control, victimization, and their influence on risky lifestyles: A longitudinal analysis using panel data. *Journal of Quantitative Criminology*, *22*(4), 319-340.

Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and psychological measurement*, *55*(5), 818-831.

Sears, D. O. (1986). College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature. *Journal of personality and social psychology*, *51*(3), 515.

Shadel, D. P., & Pak, K. B. S. (2007). The psychology of consumer fraud. *Unpublished PhD dissertation, Tilburg University*. Available online at: https://www.taosinstitute.net/Websites/taos/files/Content/5693790/Pak.ShadelDissertationFINAL.pdf (Accessed 20th January 2018).

Silvia, P. J. (2005). Deflecting reactance: The role of similarity in increasing compliance and reducing resistance. *Basic and Applied Social Psychology*, *27*(3), 277-284.

Slovic, P., & Peters, E. (2006). Risk perception and affect. Current directions in psychological science, 15(6), 322-325.

Smith, R. G. (1999). Fraud and financial abuse of older persons. *Current Issues in Crim. Just.*, *11*, 273.

Smith, R. G. (2010). Identity theft and fraud. *Handbook of internet crime*, 273-301.

Snyder, C. R., & Larson, G. R. (1972). A further look at student acceptance of general personality interpretations. *Journal of Consulting and Clinical Psychology*, *38*(3), 384.

Snyder, C. R., & Newburg, C. L. (1981). The Barnum effect in a group setting. *Journal of personality assessment*, *45*(6), 622-629.

Snyder, C. R., & Shenkel, R. J. (1976). Effects of" favorability," modality, and relevance on acceptance of general personality interpretations prior to and after receiving diagnostic feedback. *Journal of Consulting and Clinical Psychology*, *44*(1), 34.

Spalek, B. (1999). Exploring the impact of financial crime: a study looking into the effects of the Maxwell scandal upon the Maxwell pensioners. *International Review of Victimology*, *6*(3), 213-230.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the ACM*, *54*(3), 70-75.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. *IT Professional*, *18*(5), 26-32.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics*. New York: Allyn & Bacon.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education*, *2*, 53.

The Fraud Act (2006)
Available online at:
https://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf
(Accessed 12th December, 2017)

Thompson, B. (2004). *Exploratory and confirmatory factor analysis: Understanding concepts and applications*. Washington, DC: American Psychological Association.

Thunholm, P. (2004). Decision-making style: habit, style or both?. *Personality and individual differences*, *36*(4), 931-944.

Titus, R.M. and Gover, A.R., 2001. Personal fraud: The victims and the scams. *Crime Prevention Studies*, *12*, pp.133-152.

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency*, *41*(1), 54-72.

Van Dijk, J. J. (2001). Attitudes of victims and repeat victims toward the police: Results of the International Crime Victims Survey. *Crime prevention studies*, *12*, 27-52.

Van Wilsem, J. (2011). 'Bought it, but never got it'Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168-178.

Walsh, M. E., & Schram, D. D. (1980). The victim of white-collar crime: Accuser or accused. *White-Collar Crime: Theory and Research, Beverly Hills (CA): Sage*.

Weatherly, J. N., Miller, K., & McDonald, T. W. (1999). Social influence as stimulus control. *Behavior and Social Issues*, *9*(1/2), 25.

Whiteside, S. P., & Lynam, D. R. (2001). The five factor model and impulsivity: Using a structural model of personality to understand impulsivity. *Personality and individual differences*, *30*(4), 669-689.

Whitty, M. T., & Buchanan, T. (2012a). The psychology of the online dating romance scam. *A report for the ESRC*. Available online at: https://www2.le.ac.uk/departments/media/people/monica-whitty/Whitty_romance_scam_report.pdf (Accessed 1st November 2017)

Whitty, M. T., & Buchanan, T. (2012b). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.

Whitty, M.T., 2013. The Scammers Persuasive Techniques Model Development of a Stage Model to Explain the Online Dating Romance Scam. *British Journal of Criminology*, *53*(4), pp.665-684.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176-194.

Workman, M. (2008). Wisecrackers: A theory‐grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the Association for Information Science and Technology*, *59*(4), 662-674.

Yan, G., Eidenbenz, S., & Galli, E. (2009, September). Sms-watchdog: Profiling social behaviors of sms users for anomaly detection. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 202-223). Springer, Berlin, Heidelberg.

Yamagishi, T., Kikuchi, M., & Kosugi, M. (1999). Trust, gullibility, and social intelligence. *Asian Journal of Social Psychology*, *2*(1), 145-161.

Yamagishi, T., & Kakiuchi, R. (2000). It takes venturing into a tiger's cave to steal a baby tiger: Experiments on the development of trust relationships. *The Management of Durable Relations*, 121-3

Zuckoff, M., (2005). "Annals of Crime: The Perfect Mark", *The New Yorker*, Vol. 82, Iss. 13, 2005, 36-42.

Appendices

List of Apendices

List of Tables

List of Figures

1.1 Ethical approvals, recruitment and debriefing supplements

1.1.1 UPR16 Form

FORM UPR16

Research Ethics Review Checklist

University of Portsmouth

Please include this completed form as an appendix to your thesis (see the Postgraduate Research Student Handbook for more information

Postgraduate Research Student (PGRS) Information				**Student ID:**	27.2.2018642257
PGRS Name:	Martina Dove				
Department:	Psychology	**First Supervisor:**		Dr Mark Turner	
Start Date: (or progression date for Prof Doc students)		**Feb 2012**			
Study Mode and Route:	Part-time ☒ Full-time ☐	MPhil ☐ PhD ☒		MD ☐ Professional Doctorate ☐	

Title of Thesis:	Predicting Individual Differences in Vulnerability to Fraud
Thesis Word Count: (excluding ancillary data)	66650

If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University's Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study

Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).

UKRIO Finished Research Checklist:
(If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: http://www.ukrio.org/what-we-do/code-of-practice-for-research/)

a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?	YES ☒ NO ☐
b) Have all contributions to knowledge been acknowledged?	YES ☒ NO ☐
c) Have you complied with all agreements relating to intellectual property, publication and authorship?	YES ☒ NO ☐
d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?	YES ☒ NO ☐
e) Does your research comply with all legal, ethical, and contractual requirements?	YES ☒ NO ☐

Candidate Statement:

I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)

Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):	SFEC 2014-067

If you have *not* submitted your work for ethical review, and/or you have answered 'No' to one or more of questions a) to e), please explain below why this is so:

Signed *(PGRS)*:	Martina Dove	**Date:** 27.2.2018

UPR16 – August 2015

1.1.2 Study 1 - Chapter 3

1.1.2.1 Ethical approval; Study 1

-

Faculty of Science
University of Portsmouth
St Michael's Building
White Swan Road
PORTSMOUTH
PO1 2DT

Date 27/11/13

FAVOURABLE OPINION

Proposal Title: Why are scammers so successful? Reflexive accounts of victims of scams.

Dear Martina,

Thank you for submitting your revised protocol for ethical review. Both the initial reviewers are satisfied with your revisions, and your application has been given a favourable opinion. Thus, no further action is required on your part.

Good luck with the study.

Best wishes,

Dr Jim Sauer
Psychology rep, Science Faculty Ethics Committee

CC -
Dr Chris Markham – Chair of SFEC
Sci.fac@port.ac.uk
psychologycourseadmin@port.ac.uk

1.1.2.2 Invitation letter; Study 1

University of Portsmouth
Department of Psychology
King Henry Building
King Henry I St. PO1 2DY

University of Portsmouth is looking for participants for a research study looking into scams.

Many people become victims of scams. With the Internet becoming a necessity for many people, scams have evolved and happen more frequently. This is because Internet allows scams to be delivered to people's homes without much effort and scammers are exploiting this in various ways. The study will consist of one interview (face to face or on the phone) and will ask questions regarding the scam, any information or details you might have been given by the scammer(s) as well as your feelings, thoughts and experiences at the time and after the scam. Information gained through these interviews will be used to explore how people process scam information and guide us in developing better scam prevention measures in the future.

We are looking for people who are 18-60 year old and who have been victims of at least one scam (internet or otherwise) where they lost or were persuaded to give money to a scammer. We would also like to hear from people who experienced communicating with the scammer but decided not to proceed.

Some examples of scams include;
- purchasing goods that never arrived and not getting your money back
- financial investments with large returns
- bogus lotteries or clairvoyant readings
- scams that promised you money for allowing your account to be used to deposit funds
- emails asking you to financially help someone in trouble

Participation is completely voluntary and your data will be strictly confidential and used only for this study. You may change your mind about participating at any point of the process, even at the interview.

If you wish to find out more, you can do so by contacting the researcher via email: martina.dove@port.ac.uk and an information pack will be sent for your consideration.

Finally, thank you for taking the time to read this letter.
Please do not hesitate to get in touch with any questions you may have.

1.1.2.3 Information sheet; Study 1

University of Portsmouth
Department of Psychology
King Henry Building
King Henry I St. PO1 2DY

The purpose of the study
The purpose of the interview is to gather information on how and why people engage with scams and this information might be used as to prevent scams in the future, such as coming up with better warnings. This may help other people to recognise the warning signs when they are being scammed.

Explanation of the procedure and what the questions will cover
The interview will take approximately 1 to 2 hours. It is hard to say exactly how long it will take as each person's experience is different, but it is unlikely to take longer than that. The interview can be done face to
face or over the telephone and it is important that you think of the time when you may be able to do it without interruptions. The interview will be audio recorded and the recording will be used for the analysis. I will ask you about the scam you were involved in and the questions I will cover are: how did you hear about the scam, what kind the information you received about the scam and what were your thoughts and feelings regarding the scam or the perpetrator and anything else regarding the scam you wish to share with me. You can stop the interview at any point without giving a reason as well as decline to answer any questions that you are not
happy to answer during the interview.

Your data
Your answers will be treated according to Data Protection Act, which means that what you say to me will be private and confidential. An audio recording of the interview is for data analysis and will be used only for this purpose. The audio recording might be used by the interviewer's supervisory team but no one else and will be stored securely in a locked cupboard. Once the audio is transcribed, the recording will be destroyed. Your name, address or any other features that may connect the audio recording or the transcript of the recording to you will not be stored with the audio recording. The data from the transcript might be written up and published in research journals but before it is published or shared in any way, it will be anonymised. This means that your name, descriptive features or anything else about you will not be used alongside the data and you will not be able to be recognised. The data gathered in this interview will be used solely for the purpose of the research and you have the right to ask for your data to be withdrawn at any time but once the results have been written up and/or published, this may no longer be possible. You will be advised of such time in advance. You may request to see written results once the research has been written up.

Approval of the research
This interview study has been reviewed by the Research Ethics Committee, Department of Psychology at University of Portsmouth and will be conducted in accordance with British Psychological Society's code of ethics.

Contact
If you wish to discuss any of the above, please contact the researcher, Martina Dove
martina.dove@port.ac.uk

1.1.2.4 Informed consent; Study 1

Name of the researcher: Martina Dove
Supervisory team: Mark Turner, Darren Van Laar
Affiliation: Deapartment of Psychology, University of Portsmouth
Purpose of data collection: Post-graduate research (PhD)
Contact details. martina.dove@port.ac.uk, mark.turner@port.ac.uk or darren.van.laar@port.ac.uk

Please read the statements below and sign and date the consent form to indicate you consent to participation in this interview study

I confirm that I have read the information sent to me prior to this interview and that I understood what the interview is about and what is expected of me and had time to consider all the information and ask any questions and all my questions have been answered.

I understand that my participation in this interview is voluntary and that, should I choose to, I can change my mind at any time. I understand that I don't have to answer any questions I don't wish to and that I don't need to give a reason.

I have been informed that an audio recording of the interview will be made and I consent to this. I consent for the recording to be used for the purpose of the research study in question and I understand that audio will be stored securely by the researcher until the results are written up and then destroyed securely. The consent form will be kept away from the recording of my interview so there is no way of recognition. I understand that the audio might be shared with the supervisory team besides the researcher.

I have been informed that I can request my recording or any data held about me to be withdrawn or destroyed. However I understand that once the results are written up and published, this will be impossible. I give consent for my anonymised data to be used for post-graduate research and published in scientific journals and I confirm that the process of making data anonymous has been explained to me.

I understand that I can contact the researcher about the results of this research or for any other queries I may have after the interview.

If you have any questions about the consent form, please ask for clarification before you sign.

Signed: _____ Date: _____

1.1.2.5 Debriefing information; Study 1

University of Portsmouth
Department of Psychology
King Henry Building
King Henry I St. PO1 2DY

Name and contact details of the researcher:
Martina Dove - martina.dove@port.ac.uk,
Names and contact details of the supervisory team:
Mark Turner - mark.turner@port.ac.uk
Darren Van Laar - darren.van.laar@port.ac.uk

Thank you so much for participating in this interview. The information collected, along with information from other people who had similar experience as yours, will be used to gain better understanding how scams draw people in and what can be done to enable people to learn to recognise scams. As there are financial and psychological implications of being a victim of a scam, sharing your experience is invaluable and will play an important part in promotion of public scam prevention messages. I hope you did not find the interview too distressing and that you feel positive about it overall.

If there is anything that you recall and would like to add to your interview or discuss with me, please do not hesitate to contact me on the above e-mail address. Equally, if you feel there was something you wish to clarify or you have any questions about the interview or the study, please contact me. You have the right to request for your data to be removed from the study 2 weeks after the interview. After this time it is likely that it may not be possible to do so if the results have already been written up but if you have doubts about this, do not hesitate to contact me and discuss your concerns to find a solution.

If you wish to see the written summary of the results, you can request this at any time and you will be kept informed and notified when this is available.

Should you have any particular concerns about the way the interview was conducted or any other concerns about the research, you should get in touch with the supervisory team using the information above. If your concerns have not been addressed, you can contact the Chair of Psychology Research Ethics Committee in writing: Chair of the Department Research Ethics Committee, Department of Psychology, King Henry I Street, Portsmouth, PO1 2DTY.

If you feel that participating in this study has affected you in a negative way or evoked painful memories or negative feelings, you can contact confidential and free counselling service available through University of Portsmouth (Phone: 02392 843157) or Samaritans (08457 90 90 90). You can also seek help from Victim support (0845 30 30 900).

Once again, I would like to thank you for participating in this research. Knowledge gained from these interviews is priceless and will aid in prevention of scams in the future.

1.1.3 Study 2 - Chapter 4

1.1.3.1 Ethical approval

Science Faculty Ethics Committee
Faculty of Science
University of Portsmouth
St Michael's Building
White Swan Road
PORTSMOUTH
PO1 2DT

Dr Martina Dove
Department of Psychology

Martina.Dove@port.ac.uk

ethics-sci@port.ac.uk

22 January 2015

Protocol Title: SFEC 2014-067, A scale development study to assess the reliability of a scam sensitivity scale
Date received PI response from Provisional Opinion Letter: 12/01/15
Date Reviewed: 20/01/15

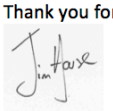
FAVOURABLE OPINION – SFEC 2014-067

Dear Dr Dove,

Thank you for your resubmission for ethical review and the clarifications provided. Having completed their review, members of the Science Faculty Ethics Committee have reached a Favourable opinion of your proposed research.

Please notify the committee of any substantial amendments to the proposed procedures, send an annual report to the committee regarding study progress and a final study report once the study has concluded. Please send these to ethics-sci@port.ac.uk.

Thank you for your submission and the Committee wish you well with your study.



Dr Jim House
Vice Chair of SFEC

Information:
Holly Shawyer - Faculty Administrator

If you would like to offer any feedback on the Science Faculty Ethics Committee process please email ethics-sci@port.ac.uk to be forwarded to the Chair

1.1.3.2 Invitation letter; Study 1

University of Portsmouth
Department of Psychology
King Henry Building
King Henry I St. PO1 2DY

INVITATION LETTER

Dear potential participant

You have been invited to participate in a short survey.

The purpose of this research study is to test and understand factors that may influence a person's vulnerability to scams (such as why people find fraudulent offers appealing). Understanding these factors is important due to the fact that scams affect so many people, who are often unable to get their money back or see their scammer jailed. In this study, we will be comparing our measure of scam vulnerability to an existing questionnaire. By participating in this study, you will be helping to design better campaigns and warnings, which may help people to avoid scams in the future.

An information sheet with more details about participating in our research can be found at the start of the survey.

We are looking for people aged 18 and over. The survey is likely to take 15-20 minutes and you can complete it in your own time by clicking the link below or by copy and pasting it into your browser

Link to survey

If you have any questions regarding the study or would like to find out more about it before you participate, please email the researcher: martina.dove@port.ac.uk

Finally, thank you for taking the time to consider participating in our study.

Martina Dove

Postgraduate Research Student

1.1.3.3 Information sheet; Study 2

University of Portsmouth
Department of Psychology
King Henry Building
King Henry I St. PO1 2DY

PARTICIPANT INFORMATION SHEET

Principal Investigator: Martina Dove Telephone: 02392 846313
Email: martina.dove@port.ac.uk
Supervisor: Mark Turner Telephone: 023 92846309 Email: mark.turner@port.ac.uk

STUDY TITLE: What psychological factors are important when interpreting scam information?

We are looking to recruit participants aged 18 and over who are currently living in United Kingdom.

What is the purpose of the study? The purpose of this research study is to learn more about the psychological attributes that are related to being vulnerable to scams. Understanding these factors is important as scams affect a growing number of people. In this study, you will be helping us to develop a new questionnaire designed to assess an individual's vulnerability to scams. Your scores on this questionnaire will be compared to an existing psychological measure and your assessment of some different scam situations. We hope to use the results of our study to promote better scam warnings.

What will happen to me if I take part?
You will first be asked to consent to participating in our study, after which the survey will begin. The survey will take approximately 15-20 minutes of your time. The survey has two parts. In Part One you will be asked to answer few questions about yourself and a set of questions designed to measure your general thoughts and feelings in different situations. In Part Two, part you will then be presented with some brief written descriptions that portray different situations in which you might be approached for offers or information. We will ask you to evaluate each description with respect to how you think you would personally respond to it and whether you have experienced similar situations in the past.

Taking part in this research is entirely voluntary. It is up to you to decide if you want to volunteer for the study. It is unlikely that you will find any of the questions embarrassing or upsetting but if you do, please remember that you don't have to answer any questions you don't want to and you can stop the survey at any time. You do not need to have previously been a victim of a scam to take part. However, if you have previously been a victim of a scam and find thinking about the experience difficult then you may wish not to take part. Some sources of help for those who have been victims of scams is provided at the end of this information sheet.

How will my responses be used?
Any individual questionnaire responses you provide will be strictly confidential and will only be seen by the researcher. When the results of our study are presented, any

responses you have contributed will not be personally identifiable to you. You will only be asked to provide a contact email address at the beginning of the survey so that we can identify you as a participant in case you later wish to contact us after taking part (for example, if you later decide you wish to withdraw your answers from the study). You will have 14 days after completion of the survey to request your data to be destroyed by emailing the researcher at the above email.

What if there is a problem?
If you have a concern about any aspect of this study, you should speak to the Principal Investigator in the first instance if this is appropriate, or the Supervisor. If you have a complaint, you can also contact:

a. The Chair of the Science Faculty Ethics Committee – Dr. Chris Markham, Chris.Markham@port.ac.uk

b. The University Complaints Officer, 023 9284 3642, complaintsadvice@port.ac.uk

The information presented above will also be repeated once you finish the survey.

Who is funding the research?
This research is not externally sponsored. None of the researchers involved with this research will receive any financial reward for conducting this study, other than their normal salary / bursary as an employee / student of the University.

Who has reviewed the study?
This study has been scientifically and ethically reviewed, and given a favourable ethical opinion by the Science Faculty Ethics Committee.

Further sources of help and information about scams
If you have been personally affected by a scam and do not wish to participate in this research then you are free to do so. If you feel that this study may affect you in a negative way or evoke painful memories or negative feelings, you can contact confidential and free counselling service available through the Samaritans (08457 90 90 90). Some sources you may contact for advice about scams are Victim support (0845 30 30 900) and Action Fraud (0300 123 2040). These contact details will also be provided again at the end of our survey.

Thank you
Thank you for taking time to read this information sheet and for considering volunteering for this study. If you wish to know more about the study before deciding, please email the researcher for further information (contact details provided at the beginning of this sheet). If you are interested in the results of the study, a summary can be sent to you once the analysis has been concluded and results written up. Please email the researcher to register your interest.

1.1.3.4 Informed consent; Study 2

INFORMED CONSENT

What psychological factors are important when interpreting scam information?
Principal Investigator: Martina Dove Email: martina.dove@port.ac.uk

STUDY DESCRIPTION: The purpose of this research study is to learn more about the psychological attributes that are related to being vulnerable to scams. Understanding these factors is important as scams affect a growing number of people. In this study, you will be helping us to develop a new questionnaire designed to assess an individual's vulnerability to scams. Your scores on this questionnaire will be compared to an existing psychological measure and your assessment of some different scam situations. We hope to use the results of our study to promote better scam warnings. You do not need to have previously experienced a scam to take part. However, if you have previously been a victim of a scam and find thinking about the experience difficult then you may wish not to take part.

FURTHER IMPORTANT DETAILS: Informed consent is routinely required for participants in psychological studies. Please read the information below before deciding whether or not to participate in this study.

1. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason.

2. I confirm that I have had the opportunity to consider the study information and understand the nature of the survey I will be asked to complete. I have had the opportunity to contact the researcher before taking part and any questions I have about the study have been satisfactorily answered.

3. I understand that the findings of this study may later be published or presented at meetings, however any individual responses I provide will not be personally identifiable to me. I give my permission for my data to be disseminated in this way.

4. I confirm that any responses I contribute can be retained confidentially and may be used in future research that has been approved by a Research Ethics Committee.

5. I understand that if I later wish my responses not to be used in the study, I will have 14 days after completing the survey to contact the researcher and request that my responses are not used in the study. After this period, it will not be possible to withdraw my data.

If you have read and understood the nature of this study and are willing to continue please tick the box below to continue with the survey

□ I agree to participate in the study.

1.1.3.5 Debriefing information; Study 2

University of Portsmouth
Department of Psychology
King Henry Building
King Henry I St. PO1 2DY

Name and contact details of the researcher: Martina Dove -martina.dove@port.ac.uk

Names and contact details of the supervisory team:
Mark Turner - mark.turner@port.ac.uk
Darren Van Laar – darren.van.laar@port.ac.uk
Alessandra Fasulo – alessandra.fasulo@port.ac.uk

Thank you so much for participating in this study.
The data gathered from this survey will aid in developing a new questionnaire measure that may be used to identify psychological factors connected to scams. The data will be used to conduct statistical analyses needed to compare this new scale with existing ways of assessing personal susceptibility to scams and explore any other, as yet unidentified factors that may be important in how we interpret scam information.

Identifying new factors connected to scam vulnerability will allow us to create better preventive measures, such as more relevant warnings for certain groups of people, or more generally, tailored communications and advice that people may find relevant and memorable. This may help victims and potential victims avoid future scams.

If after participating, you feel you do not wish your data to be used, you may request your data to be deleted from the study for up to 14 days by contacting the researcher using the contact email provided above, after which time it will no longer be possible for us to withdraw your data from the study.

If you would like a written copy of this debriefing information or would later wish to receive a summary of our findings once the study is complete these can also be requested by contact the researcher.

Should you have any particular concerns about this research, in the first instance you may contact the researcher's supervisor Dr. Mark Turner via email: mark.turner@port.ac.uk or in writing: Department of Psychology, King Henry I Street, Portsmouth, PO1 2DY.

If your concerns have not been addressed, you can contact the Head of the Psychology Department Dr. Sherria Hoskins, Head of the Department of Psychology, King Henry I Street, Portsmouth, PO1 2DY. Or Tel. 02392 846313.

If you feel participating in this study has affected you in a negative way, you can contact a confidential and free counselling service available through the University of Portsmouth (Phone: 02392 843157 - for students only) or the Samaritans (08457 90 90 90 - for other participants). For further help or advice about specific scams you can also contact Victim support (0845 30 30 900) and Action Fraud (0300 123 2040).

1.1.4 Study 3 - Chapter 5

1.1.4.1 Ethical approval

Science Faculty Ethics Committee
Science Faculty Office
University of Portsmouth
St Michael's Building
White Swan Road
PORTSMOUTH
PO1 2DT

T: 023 9284 3379
ethics-sci@port.ac.uk

Ms Martina Dove
School of Psychology
University of Portsmouth

Martina.Dove@port.ac.uk

18 July 2016

FAVOURABLE ETHICAL OPINION – WITH CONDITIONS

Study Title: An online questionnaire study of respondents perceptions of the accuracy of personality test feedback.

Reference Number: SFEC 2016-062

Date Submitted: 30 June 2016

Thank you for submitting your protocol to the Science Faculty Ethics Committee (SEFC) for ethical review in accordance with current procedures[1].

I am pleased to inform you that SFEC was content to grant a favourable ethical opinion of the above research on the basis described in the submitted documents listed at Annex A, and subject to standard general conditions (*See Annex B)*, and the following specific minor conditions.

Conditions

- 11.4 states that data 'may be retained for ten years, may be used'.....please specify the actual intention.
- Debriefing-the escalation path is incorrect.
- debriefing 'Are aim' should read 'our aim'.
- please show actual demographic capture questions that will be asked (Appendix B).
- Complaints should be made to HoD Sherria Hoskins rather than the Chair of SFEC.

If you would find it helpful to discuss any of the matters raised above or seek further clarification from a member of the Committee, you are welcome to contact ethics-sci@port.ac.uk who will circulate your queries to SFEC

Please note that the favourable opinion of SFEC does not grant permission or approval to undertake the research. Management permission or approval must be obtained from any host organisation, including the University of Portsmouth or supervisor, prior to the start of the study.

Wishing you every success in your research

[1] Procedures for Ethical Review, Science Faculty Ethics Committee, University of Portsmouth, October 2012 (to be updated).

1.1.4.2 Invitation letter

University of Portsmouth
Department of Psychology
King Henry Building
King Henry Street, PO1 2DY

Principal Investigator: Martina Dove
Telephone: 023 9284 6313
Email: martina.dove@port.ac.uk
Supervisor: Mark Turner
Telephone: 023 9284 6309
Email: mark.turner@port.ac.uk

Study Title; An online questionnaire study of respondents' perceptions of the accuracy of personality test feedback.

You are invited to take part in a research study looking into perceptions of accuracy of personality test feedback. The survey takes approximately 20-30 minutes and anyone over 18 is welcome to participate. You will first be asked to answer questions about your attitudes and daily activities, after which you will be presented with your personality feedback. Since we are trying to assess if the personality perception questionnaire is accurate in delivering personality feedback, you will be asked to rate this feedback sentence by sentence on a 1-10 accuracy scale.

SURVEY LINK

When you click on a survey link, you will be provided with more detailed information about the study. If you have any questions before the survey, or require further information, please email the principal investigator; martina.dove@port.ac.uk

1.1.4.3 Information sheet

University of Portsmouth
Department of Psychology
King Henry Building
King Henry Street, PO1 2DY

Principal Investigator: Martina Dove
Telephone: 023 9284 6313
Email: martina.dove@port.ac.uk
Supervisor: Mark Turner
Telephone: 023 9284 6309
Email: mark.turner@port.ac.uk

Study Title: An online questionnaire study of respondents' perceptions of the accuracy of personality test feedback.

What is the purpose of the study?
The purpose of this study is to help develop a new personality questionnaire, by allowing us to examine how people perceive the accuracy of feedback they receive about their personality characteristics from the test we are developing.

What will happen to me if I take part?
Taking part in this research is entirely voluntary. It is up to you to decide if you want to volunteer for this survey.

In the first part you will answer questions about your daily attitudes and behaviours. This part of the study will take around 20 minutes to complete. You will then be given feedback about your personality based on the questionnaire responses you have provided. We will ask you to rate each element of this feedback with respect to how true you feel it is of you, in order to see how effective our questionnaire is at producing accurate feedback. This part of the study will take around 10 minutes to complete. The study will also ask you to provide some brief demographic information about yourself. Overall, the survey is likely to take around 30 minutes to complete, after which nothing further is needed on your part.

You will be asked to indicate that you wish to take part in the study below, prior to starting the survey. It is not necessary for you to provide your personal name or contact details in order to take part. During the study, you will be asked to create a username. If you later decide you would rather not take part, you may stop the survey at any time. You may also request that any data you have provided be withdrawn from the study for up to 14 days after participation, by contacting the researcher and quoting the unique username that you created as part of the study.

Your data will be treated confidentially, and will be kept secure at all times in an encrypted file stored on a password protected computer account. Your responses will be added to those of other people and used only as a part of a large data analysis. The anonymised data set may be kept for future psychological research that has been approved by a research ethics committee. The results of this study are also likely to be

disseminated through publications, meetings and conferences. However, at no point will your personal details be shared with anyone apart from the research team.

What are the possible disadvantages and benefits of taking part?
We do not foresee any risks connected to taking part in this study, and you may stop participating at any time should you wish to do so. It might be possible that you will feel some of the feedback you will receive is not a fair description of you, or does not paint you in a good light, which might have the potential to cause upset. It is important to remember that we are still in the process of refining the feedback produced and that you will also have the opportunity of giving your view on the accuracy of the feedback you receive. Psychologists are always looking for ways to understand and assess personality characteristics better and you will be contributing to the research in this area as well as getting personalised feedback after completion.

Who is funding the research?
This research is not externally sponsored. None of the researchers involved with this research will receive any financial reward for conducting this study, other than their normal salary / bursary as an employee / student of the University.

Who has reviewed the study?
This study has been scientifically peer reviewed within the Department of Psychology, and ethically reviewed by the Science Faculty Ethics Committee, receiving a favourable ethical opinion.

What if there is a problem?
If you have a query, concern or complaint about any aspect of this study, in the first instance you should contact the Principal Investigator (PI) or her Supervisor, using the contact details given above. If you concern is not addressed, or you wish to make a complaint about the study, you can also contact:

a. Dr. Sherria Hoskins, Head of department, 023 9284 6321, sherria.hoskins@port.ac.uk

b. The University Complaints Officer, 023 9284 3642, complaintsadvice@port.ac.uk

Thank you for taking time to read this information and for considering volunteering in our research. If you do not wish to participate you may close the survey now. If you do wish to take part in our study your formal consent will be sought on the following page of the survey.

1.1.4.4 Informed consent

INFORMED CONSENT

Please read the information provided about this study carefully, before continuing.

Participation in this survey is voluntary and you are free to withdraw at any time without giving any reason, even after the full completion of the survey. The survey will not ask you to supply any personal details apart from your gender and age, and you will not be asked to supply any personal contact details that would otherwise identify you.

Whilst some information that could identify you (such your computer's IP address may be automatically logged during the survey, at no time will we release or make use of this information, and once each participant's responses have been collected this information will be deleted.

Your individual questionnaire responses will not be used on their own, instead they will be combined with responses from other participants. These data, will be made anonymous (i.e. free of any features that may identify you personally), and stored for at least 10 years within the university, in accordance with the university's Retention Schedule for Research Data. The results based on this data will be written up and published in academic journals and/or presented at academic conferences and meetings. The anonymised data may also be used as part of a future research study that has been approved by a Research Ethics Committee.

If you require any further information before deciding whether to participate, you may email the researcher (martina.dove@port.ac.uk) to request more details before you take part.

Please tick each statement below before continuing to the survey questions.

- ☐ I confirm that I have read and understood the study information for the above study.
- ☐ I confirm that I have had the opportunity to consider this information, ask questions and that any questions I had, have been answered satisfactorily.
- ☐ I agree to participate in the study.

1.1.4.5 Debriefing information

University of Portsmouth
Department of Psychology
King Henry Building
King Henry Street, PO1 2DY

DEBRIEFING INFORMATION

Principal Investigator: Martina Dove
Telephone: 023 9284 6313
Email: martina.dove@port.ac.uk
Supervisor: Mark Turner
Telephone: 023 9284 6309
Email: mark.turner@port.ac.uk

Thank you so much for taking the time to participate in this study. Please read the following text below as it contains important information about the study you just participated in.

What was the purpose of this study?
The purpose of this research study was to learn more about the psychological attributes that are related to fraud susceptibility and whether these can be predicted. This study was designed to test a newly developed questionnaire against a potential scam situation, in order to see if the questionnaire could accurately predict responses. Identifying new factors connected to scam vulnerability will allow us to create better preventive measures, such as more relevant warnings for certain groups of people, or more generally, tailored communications and advice that people may find relevant and memorable. This may help victims and potential victims avoid future scams. As such, during this survey we created a situation to mimic the psychological conditions of a scam, which it was not possible to tell you about prior to taking part in the study in order to avoid biasing the answers you provided. We apologise for temporarily misleading you regarding the nature of the study. If, after considering the information below you feel affected by this, several sources of help and advice are provided at the bottom of this page.

How did the study work?
In this study, you completed three questionnaires designed to assess personality attributes related to fraud susceptibility, a measure of "locus of control" (or the extent to which individuals believe they can control events affecting them) and a measure of psychological compliance. Following the completion of the scales you were shown feedback which we indicated was based on your personal responses. In fact, every person who takes part in our study was given the same feedback consisting of neutral, positive and negative statements. Our aim was to identify whether people with certain psychological attributes (as measured by the three questionnaires you completed) were more or less likely to believe the general feedback that was given to them.

Previous studies have suggested that people find generalised neutral statements to be highly credible and believe them to be accurate personality feedback, whereas these statements are vague and can broadly apply to everyone. This situation (asking people to respond to plausible but false information) is often exploited in scams that involve cold readings, such as clairvoyant scams.

Studies have found that people also believe positive statements to be very true of themselves and negative statements to be more applicable to other people than themselves. We are interested in examining whether people who hold overly positive view of themselves also tend to exhibit specific scam vulnerability characteristics.

Feedback and withdrawing your data
We would also like to hear any feedback you might have on how this study affected you. This feedback is not part of the study but is extremely valuable and may be used to discuss potential harm to participants where the true nature of the study cannot be revealed at the start and to aid designs of studies in the future.

If after considering the above information, you do not wish your data to be used in the study, you may request to withdraw your responses (for up to 14 days) after you completed the survey. You do not need to give a reason for this. If you would like to request your responses to be removed, please tell us in the box below, or (afterwards) by contacting the Principal Investigator via the email address shown above and quoting the unique username you created during the study.

Please use the box provided to leave the feedback, if any or to request your data to be removed.

Complaints
If you have a query, concern or complaint about any aspect of this study, in the first instance you should contact the Principal Investigator (PI) if appropriate *or the Supervisor*.
Both contact details are listed above.

If you have a concern about any aspect of this study, you should speak to the Principal Investigator in the first instance if this is appropriate, or the Supervisor. If you have a complaint, you can also contact:

a. Dr. Sherria Hoskins, Head of department, 023 9284 6321, sherria.hoskins@port.ac.uk

b. The University Complaints Officer, 023 9284 3642, complaintsadvice@port.ac.uk

If you feel distressed and need further help
If you feel participating in this study has affected you in a negative way, you can contact a confidential and free counselling service available through the University of Portsmouth (Phone: 02392 843157 - for students only) or the Samaritans (08457 90 90 90 - for other participants).

For further help or advice about specific scams you can also contact Victim support (0845 30 30 900) and Action Fraud (0300 123 2040).

Thank you for participating in this research study
If you are interested in the results of the study, a summary can be sent to you once the analysis has been concluded and results written up. Please email the researcher to register your interest.

As a thank-you for taking part in this research, we would also now like to provide you with some genuine personality feedback based upon the Locus of Control Scale and Compliance scales you completed during this survey. Your individual scores on these two questionnaires together with an overall explanation of which each of these scales indicate is provided on the next page.

CLICK HERE TO RECEIVE PERSONALITY FEEDBACK

1.2. Ethical considerations and sampling criteria

Table 1.1
Ethical considerations and sampling criteria for Study 1, Chapter 3

Sampling exclusions	
Exclusion criteria	**Rationale for exclusions**
Participants under 18 years of age, those with mental illness and over 65 years of age were excluded	Research argues that the reason elderly people are more aggressively targeted by scammers is due to diminishing cognitive functions that can be part of an ageing process (Langenderfer & Shimp, 2001; Callahan et al., 2002; Griffiths & Harmon, 2011) as well as other factors related to old age, such as loneliness and loss of independence (Martin, 2009). The study's aim was to explore cognitive and motivational factors underlying the processing of scam information. As such, interviewing individuals over 60 might have unearthed confounding factors to this process. Participants with mental impairments, participants under 18 or those with mental illness were also excluded due to their vulnerability as outlined by BPS code of ethics.
Romance scams were excluded	Romance scams were extensively covered in recent research (Witty, 2013; Witty & Buchanan, 2012; Buchanan & Witty, 2013). In addition, romance scams follow a different path to scams that require careful consideration of the scam message. In addition, romance scams were found to cause victims great distress so any recollection of this event for research purposes, unless necessary, might have caused further distress.
Ethical considerations	
Informed consent	Participants were given the information sheet on the nature of the study prior to the interview and were encouraged to ask questions if they wanted to know more. Each participant was reminded at the start of the interview that they can terminate the interview at any time and/or request for their data to be removed from the study without any further obligation. Participants interviewed face-to-face were asked to sign a consent form and participants interviewed over the phone were read the consent form and asked if they agreed and their consent recorded.
Confidentiality	Participants data was made anonymous during transcription by changing all names, as well as names of places and organisations mentioned (if referring to participant's life). Recordings of the interviews were destroyed after the transcribing was completed. Consent forms were kept in a locked cupboard within the Department of Psychology and only the researcher had access to participants' contact details.
Minimising harm and discomfort to participants	The study was advertised so that anyone wishing to participate would As the nature of the topic was sensitive, we anticipated some participants would feel distress at recollection of events. Participants were asked about their feelings and emotions during the recollection of the events and if anything could have been done differently by the researcher to minimise the distress. Participants received a full debrief with sources of support for victims of fraud as well as counselling services. In addition, participants were offered the choice of the interview setting, either face-to-face (at the location of their choosing, which included the university, participant's home or workplace or a public place) or over the phone, in order to make them feel as comfortable as possible during the interview. All participants were also offered a summary of findings.

Table 1.2
Ethical considerations and sampling criteria for Study 2, Chapter 4

Sampling exclusions	
Exclusion criteria	**Rationale for exclusions**
Participants under 18 years of age	Participants under 18 were excluded due to their vulnerability as outlined by BPS code of ethics.
Ethical considerations	
Informed consent	Consent information was embedded within the survey for participants to consider before commencing the survey. Participants were asked to confirm their agreement to take part through a response item shown after the consent information.
Confidentiality	The survey was confidential and we encouraged participants to only leave their email address if they feel they may want to withdraw their data at the later date. IP addresses of participants were deleted as soon as the survey closed and data was converted into a data set. Participants were not asked for their names and data was only used as a part of a large data set.
Minimising harm and discomfort to participants	The survey contained questionnaires that pertained to scams, which may have been distressing to those who were defrauded in the past. A reminder was included in the consent information informing participants that they may potentially feel embarrassed or distressed if they experienced fraud victimisation in the past, and if they feel this may be the case, they are free to change their mind at any point and withdraw from the survey. In addition, participants received a full debrief with sources of support for victims of fraud and further information about scams and agencies that scams can be reported to.

Table 1.3
Ethical considerations and sampling criteria for Study 3, Chapter 5

Sampling exclusions	
Exclusion criteria	**Rationale for exclusions**
Participants under 18 years of age	Participants under 18 were excluded due to their vulnerability as outlined by BPS code of ethics.
Ethical considerations	
Informed consent	Consent information was embedded within the survey for participants to consider before commencing the survey. Participants were asked to confirm their agreement to take part through a response item shown after the consent information.
Confidentiality	The survey was confidential and we encouraged participants to only leave their email address if they feel they may want to withdraw their data at the later date. IP addresses of participants were deleted as soon as the survey closed and data was converted into a data set. Participants were not asked for their names and data was only used as a part of a large data set.
Deception	As the study utilised deception, by utilising Barnum effect paradigm as a proxy scam situation, the true nature of the study could not be revealed to participants prior to participating. The Barnum effect studies rely on the deception (Forer, 1949; Furnham & Varian, 1988), a necessary part of the approach to ensure that true assessments of statement accuracy can be obtained. Instead participants were told they would be assessing their own personal feedback, based on the scores of psychometric tests they completed. The ethical implications of this methodology have been considered by Beins (1993) with respect to the impact of the deception on participants. The author found that when participants were appropriately debriefed, the number of objections was low, once the nature of the study was explained and any distress expressed by respondents was short-lived.
Minimising harm and discomfort to participants	Due to deception, it was anticipated that participants would experience some level of distress, once they receive a debriefing. Therefore time was taken to explain the importance of the study and how it relates to fraud research and prevention. Since participants were promised personalised feedback when consenting to take part at the beginning of the study, they received their own genuine feedback on one of the psychometric measures they completed. This was done in order to offset any disappointment participants might have experienced once the true nature of the study was revealed. In addition, participants were encouraged to leave a feedback about how the deception affected them and there were no adverse effects noted, once we considered this feedback.

1.3. Supplements for Chapter 3, Study 1

Table 1.4
Reporting path avenues and outcomes experienced by a victim of fraud interviewed in Study 1, Chapter 3

Authority body	Response	Outcome
County court	Scammer cannot be reached due to registering fake company details.	Additional loss of funds for a court fee.
Local Trading Standards	Helpful response, investigated the scammer's company address.	Due to false details given, they could not do anything more as the scammer has no presence in the borough.
Action Fraud	Raised a claim and added to the details on several occasions	Heard nothing from action Fraud and no action taken.
Local police station	Told procedures cannot be broken and to go back to Action Fraud. Police officer tried to call Action Fraud on his behalf without success.	No outcome.
National Fraud Authority	Told that he must go back to Action Fraud.	No outcome.
Action Fraud raised a formal complaint due to no response	Acknowledgement email specifying he will get a response in 20 days.	No outcome.
Action Fraud escalated the previous complaint	Acknowledgement letter specifying he will get a response in 20 days.	No response in the given time but received an email saying his case was lost but that the data will be restored.
City of London Police because he was dissatisfied with Action Fraud	Polite and helpful response but told procedures have to be followed and referred to Action Fraud.	No outcome.
VAT office reported the scammer was using fake VAT number	Noted the details.	Requested the victim to pay the VAT he reclaimed on the scam purchase, no further contact regarding the fraudulent details.
Companies House reported the scammer was registered with fictional details	Told Companies House does not check the information and that he should report it to the police.	Told to repay VAT he claimed for the fraudulent transaction.
Trading standards when he finally managed to track the scammer's address to that borough	Attempted several several phone calls and told that someone will call back to discuss.	No reply.
Action Fraud reissued formal complaint regarding the case for the second time	Acknowledgement letter specifying he will get a response in 20 days.	No further response.

Authority body	Response	Outcome
Action Fraud escalated the complaint again	Acknowledgement letter specifying he will get a response in 20 days.	No further response.
Contacted two MPs in order to take his case to Parliamentary and Health Ombudsman	First MP did not reply, the second MP was helpful.	Submitted the complaint against Action Fraud.
Parliamentary and Health Ombudsman (PHSO)	Told he will be given a decision within 16 weeks on whether they will look into the case.	No response from PHSO but contacted by a researcher and asked to give an opinion on his satisfaction regarding the fact that his case was closed - the victim was not told his case was closed by PHSO until that time.
Victim speaks to the PHSO researcher about his experience	Not applicable	Receives the call from the Metropolitan Police.
Victim receives a call from the Metropolitan Police	Police advise that the case is 2 year old now and the evidence is stale.	Told no further action will be taken and advised to go to civil court, the first step he started with.

Notes.

MP - Member of Parliament

PHSO – Parliamentary and Health Service Ombudsman

VAT – Value added tax

1.4 Supplements for the pilot study for Study 2, Chapter 4

Table 1.5
Mean item relevance ratings on a concept for the initial 56 items

	Ratings on a concept	
Question	***M***	***SD***
1. I often find myself in difficult situations I can't think how to get out of.	7.38	2.20
2. I am responsible for deciding what happens to me in every situation.	7.33	2.30
3. I normally avoid making decisions when I am feeling anxious.	7.72	2.47
4. I tend to make bad decisions when I am unhappy. *	7.16	2.53
5. I don't like surprises.	5.97	2.42
6. I tend to feel unsettled by forceful people. *	8.29	2.42
7. I normally give in when people pressure me to make a decision.	9.37	2.06
8. I prefer to take my time to think things through.	7.86	2.64
9. I avoid making decisions if someone is pressing me to choose.	7.84	2.59
10. I am always suspicious of people who ask me to make quick decisions.	8.47	2.36
11. I usually find it easy to agree with others in a group.	7.53	2.59
12. People tell me I am easy to persuade.	8.69	2.52
13. I always do what I think is best, even when I am in the minority.	7.75	2.27
14. I often find myself agreeing to things I don't really want to do.	9.14	1.95
15. I have been talked into buying something I didn't really want.	8.86	2.43
16. I always check the small print.	8.06	2.94
17. I find it hard to say no to people without seeming rude.	9.20	2.27
18. I often worry about disappointing people.	7.97	2.66
19. I find it easier to lie than say I don't want to do something.	7.46	2.36
20. I would prefer to be impolite rather than agree to something I don't want to do.	7.83	2.84
21. I am self-reliant.	6.94	2.49
22. It's not important to read all of the details before making important decisions.	8.54	1.96
23. I prefer to read contracts for myself rather than believe what others tell me is in them.	8.46	1.99
24. I often seek advice from friends and family before making financial decisions.	8.63	2.16
25. I never bother double-checking terms and conditions.	8.77	1.92
26. I prefer to get decisions over with quickly.	7.77	2.47
27. I feel others often take advantage of me.	8.34	2.27
28. I find it hard to tell if someone can be trusted.	8.09	2.11
29. I often double-check what other people tell me.	8.34	2.09
30. I usually give others the benefit of the doubt.	8.20	1.98
31. I feel safe from becoming a victim of crime.	8.14	2.60
32. Only gullible people fall for scams. **	7.34	2.97
33. I believe criminals usually end up getting what they deserve.	5.66	3.07
34. Scammers and fraudsters normally will get caught in the end. **	6.03	2.79
35. The Authorities, overall are effective at protecting us from crime. **	6.80	3.13
36. People tell me I sometimes make rash decisions.	7.86	2.56
37. When I behave impulsively, I normally end up regretting.	7.26	2.58
38. I don't like to rush my decisions.	7.80	2.45
39. I find it hard to say 'no' to people I like.	8.69	2.39
40. I tend to believe people I feel I connect with.	8.80	1.95
41. I have made mistakes when trusting people in the past.	8.66	2.11
42. I tend to only buy from companies and brands that I know.	7.71	2.65
43. I am always careful to check that emails and websites are real.	8.97	2.48
44. You can never be sure if emails and websites are real.	8.86	2.33
45. I am always careful to check out people and companies if I haven't bought from them before.	8.60	2.34
46. When something seems too good to be true, it usually is.	8.23	2.65
47. I feel compelled to act immediately when I see a bargain.	8.60	2.02
48. I get a buzz from buying new things.	7.63	2.56
49. I am prepared to take a risk when buying something I really want	8.34	2.17

	Ratings on a concept	
Question	***M***	***SD***
50. If I like something, I have to have it straight away.	7.83	2.19
51. I'm always careful to think rationally about the things I buy.	8.54	2.12
52. I find it hard to contain my excitement when lucky things happen to me.	7.40	2.28
53. People sometimes tell me that I am cynical.	7.29	2.55
54. I often try to set myself rules to avoid repeating mistakes.	7.26	2.54
55. I try hard to understand the reasons for any mistake I make.	7.14	2.45
56. When I make a mistake, I don't like to dwell on it.	6.80	2.68

Notes.
* Reworded based on feedback from the original sentence: When things are not going right in my life I often make decisions I later regret and Forceful people make me uneasy
** Questions 32, 34 and 35 were kept in order to see if belief in justice and belief that scam victims are responsible for their demise would influence fraud vulnerability

Table 1.6
Participants' comments for questionnaire items evaluated in the Pilot study, Study 2, Chapter 4

Question	**Comment**
1. I often find myself in difficult situations I can't think how to get out of.	1. If people are sucked in to a scam they find it difficult to admit they are being scammed and carry on with the scam as a means of trying to get out of it (ex) 2. If people are sucked in to a scam they find it difficult to admit they are being scammed and carry on with the scam as a means of trying to get out of it (ex) 3. The ever increasing complexity of scams lead to individuals finding themselves in situations that perhaps they cannot equate as to what has happened. (ex) Not being able to get away from tradespeople without appearing rude is something they 'prey upon! (ex) 4. I think this question is relevant to some scam victims but not all. (ex) 5. Good open question (ex) 6. Nowadays there are many resources an individual can access to assist. Also what type of situation? Physical Threat, mental stress, financial? (ex) 7. The statement implies permanency, whereas being a scam victim could be a one-off, surprise event. (vs) 8. I would interpret this statement as relating to an on-going process, repeated frauds or recovery fraud where the victim is trying to make back their losses. (ex) 9. The word "often" is very subjective (ex) 10. Some scam victims may not be as vulnerable as the question suggests (ns)
2. I am responsible for deciding what happens to me in every situation.	1. I don't think this one is relevant at all to susceptibility in my experience (ex) 2. Important in determining if person living alone or the level of support network (ex) 3. More and more automated systems are being used, so how much responsibility an individual has is a moot point (ex) 4. I do feel that personal responsibility plays a role in perceiving fraud. I would feel slightly reckless if I knew I fell for a scam. (rs) 5. Not every situation's outcome depends on our actions. We can sure decide what happens to us, but if that actually happens sometimes does not depend on our decision. (vs) 6. The use of the term 'topic' is generally confusing you should be more specific about what you want me to assess for susceptibility to scams. I guess that in this case you mean 'being responsible for deciding what happens to me. (vs) 7. I agree that the issue of personal responsibility is important but I wonder if it will resonate with victims of crime. (ex) 8. "Every" is absolute - and no-one is totally in control of what happens to them all the time (ex)
3. I normally avoid making decisions when I am feeling anxious.	1. Quite a lot of scams rely on people being under pressure, either financially or social responsibilities (i.e. parenthood) (ex) 2. Being scammed would no doubt make an individual anxious, by avoiding a decision it could be swept under the carpet. (ex) 3. Somewhat relevant, but only to a small number of people. (ex) 4. A good protective quality to have. (rs) 5. We know decision making abilities are affected when we are anxious and/ or depressed so this is a very relevant question in this context. I'm glad you said "feeling" anxious rather than just "anxious" (rs) 6. See previous comments do you mean making decisions when anxious or avoiding making decisions when anxious (vs)

Question	Comment
4. I tend to make bad decisions when I am unhappy.	1. Somewhat relevant but again to a small number of potential victims (ex) 2. Not relevant as we probably all do this if honest not just scam victims (ex) 3. With fraud/scams how much emotion is actually involved in the act. I'd say from experience very little, other than greed (ex) 4. Feedback on this item reflects feedback on the last item. (no 5 previous question) (rs) 5. Making decisions when unhappy or making bad decisions when unhappy (vs) 6. I can see the logic of trying to determine if the victim is in a hold or cold state but is that the same as being 'unhappy'? (ex)
5. I don't like surprises.	1. Not relevant (ex) 2. A big lure for scam victims, makes them feel wanted! (ex) 3. Surprises is too broad, they can be good or bad. Being surprised with a bunch of flowers always good. A surprise trip to the cinema can be bad if you are tired. (ns) 4. See previous comments what is the topic - surprises or not liking surprises (vs) 5. I'm not sure what you hope to infer from a response to this. (ex) 6. Hard to see what correlation you are looking for - do u ask if a dislike of surprises makes someone susceptible to scams? (vs)
6. I tend to feel unsettled by forceful people.	1. Once people are hooked they find it difficult to get out of the situation if the scammer dominates the communication (ex) 2. Depending on the nature of the scam it is probable that a 'face to face' scam may unsettle and convince the individual into making a decision that they wouldn't otherwise have made. (ex) 3. Highly relevant. This is a classic tactic used by some social engineers to emotionally unsettle their victims. (ex) 4. I could guess that people who are upfront, forceful and persuasive are unsettling to people susceptible to a scam. (rs) 5. Reflects my own image of scam victims being overwhelmed by persuasion, without thinking. (vs) 6. Interesting, as I would suspect that most fraudsters are forceful (ex)
7. I normally give in when people pressure me to make a decision.	1. Again they find it difficult to get out of it (ex) 2. Highly relevant again points to classic victim susceptibility when being socially engineered. (ex) 3. Maybe re-phrase - I normally say yes when people ... (ex)
8. I prefer to take my time to think things through.	1. If people have time to think things through they aren't likely to fall for most scams (ex) 2. Again this person is potentially liable to a forceful or assertive scammer (ex) 3. Comes back to the automatic versus the controlled decision making processes... have you considered that many people will see themselves as controlled but act in an automatic fashion. (ex)
9. I avoid making decisions if someone is pressing me to choose.	1. This person won't be susceptible to scams. (ex) 2. If they back off when pressured they are less likely to go with the scam (ex)
10. I am always suspicious of people who ask me to make quick decisions.	1. Again if you go into something thinking it's suspicious you are less likely to carry on with it (ex) 2. This is a good question because even suspicious people can still be conned. (ex)

Question	Comment
11. I usually find it easy to agree with others in a group.	1. Peer pressure is used a lot to coheres people into going with a scam (ex) 2. This person is susceptible to social proof and could easily be scammed. (ex) 3. Better to word it as generally find myself vying in to agreeing with others in group (easy to agree is ambiguous) (rs) 4. I feel that people who fall for scams would "go along with a group" more often than others. (rs) 5. Being carried along by the crowd, wanting to be part of a group could make people make silly decisions (ns) 6. If scams involve large groups of people (vs)
12. People tell me I am easy to persuade.	1. Obviously someone who is liable to being scammed. (ex) 2. Depends upon level of self awareness (ex)
13. I always do what I think is best, even when I am in the minority.	1. If people don't go with the flow of a scam they tend to drop off (ex) 2. This person isn't liable to social proof but could still be scammed by a persuasive conman who convinces them they are doing the right thing. (ex) 3. Not sure if/how relevant (ex) 4. Not a good question, in what context is minority being used (ex) 5. would be interesting to see if this statement reflects stubbornness or reflectiveness? (vs) 6. I can see what you're getting at... cognitive bias (ex) 7. "Always" is a bit too strong, maybe "typically" or "generally" (ex)
14. I often find myself agreeing to things I don't really want to do.	1. If you are speaking before thinking you are right up there (ex) 2. Classic (ex) 3. Better would be 'i tend to follow the general consensus' (ex) 4. Question is important in my opinion. (rs)
15. I have been talked into buying something I didn't really want.	1. Top level victim for scammers (ex) 2. Classic vulnerability (ex) 3. Similar to previous question? (ex) 4. Maybe specify - financial products or goods (ex)
16. I always check the small print.	1. The small print always gives scams away (ex) 2. This person is much less likely to be a victim. (ex) 3. Very important to avoid scams and sharp practice (ex) 4. Unsure about the literature on people who fall for scams and attention to detail. (rs) 5. Some people may need an example of what small print is. (ns) 6. Will people be honest? (ex)
17. I find it hard to say no to people without seeming rude.	1. Again if you are not looking for reasons to say NO you're more likely to say YES (ex) 2. Classic victim (ex) 3. Maybe add a scenario - 'When i am in a shop, I find it hard to... (ex) 4. the weak gullible, right? (vs)
18. I often worry about disappointing people.	1. This would imply a prior relationship so people don't tend to think it when it's a stranger (ex) 2. Classic victim very vulnerable to being scammed (ex)

Question	Comment
19. I find it easier to lie than say I don't want to do something.	1. If you don't care about what you're saying the scammer finds it difficult to follow their script and can't finish the scam (ex) 2. This person maybe able to avoid being conned. (ex) 3. Not sure how honest people would respond to this question if asked openly (ex) 4. Being strong in saying no requires strength of character, but consistently and convincingly maintaining a lie also requires strength of character, so I'm not quite sure which way this question is heading! (ex)
20. I would prefer to be impolite rather than agree to something I don't want to do.	1. Chances are you wont' be scammed (ex) 2. Resilient person. (ex) 3. This and previous few questions imply an exchange of goods/services - If it is something personal, does the same apply? (ex)
21. I am self-reliant.	1. Could go either way, either resilient or susceptible through arrogance (ex) 2. I wonder whether victims of different types of scams would answer this differently. You can be self-reliant, but still be tricked, but the type of trick may vary.(vs) 3. Self reliant? (ns)
22. It's not important to read all of the details before making important decisions.	1. Good - refers to previous question about small print (ex) 2. Laying themselves open to a fall. (ex) 3. I think that most people do read all the available details (or at least THINK they have). You might get a false high score for this question as it does not mean that they DO read all details.(rs) 4. The word "important" twice in the sentence makes it a bit clumsy (ex)
23. I prefer to read contracts for myself rather than believe what others tell me is in them.	1. Good behaviour (ex) 2. Good - this is when a person can be scammed (ex) 3. I know several people who ask others to read over contracts and agreements and 'summarise' it for them. (rs) 4. attention to detail - presumably an asset if you don't want to be tricked. (vs)
24. I often seek advice from friends and family before making financial decisions.	1. Good behaviour (ex) 2. Very general question - giving yes or no answer doesn't highlight any factor (ex)
25. I never bother double-checking terms and conditions.	1. that's where the scam normally is (ex) 2. Risky behaviour (ex) 3. Who reads the fine print? (rs) 4. attention to detail and a fair dose of suspicion? (vs) 5. "Never" is absolute (ex)
26. I prefer to get decisions over with quickly.	1. if you don't think things through you can't see the scam (ex) 2. Risky again (ex)
27. I feel others often take advantage of me.	1. Difficult because if you know people take advantage of you, you're more likely to go into the detail a bit more (ex) 2. Susceptible (ex) 3. I am not sure a fraud/scam victim would know if they were being scammed/defrauded (ex) 4. Requires self awareness (ex)

Question	Comment
28. I find it hard to tell if someone can be trusted.	1. We all find it hard to tell if someone can be trusted until we build a relationship with them (ex) 2. Stuffed if you can't do this. (ex) 3. Trust is very important to consider. (rs)
29. I often double-check what other people tell me. How important is this question as a factor in sus...	1. Desirable behaviour (ex)
30. I usually give others the benefit of the doubt.	1. Not always wise. (ex) 2. I don't understand the question. Language problem. (ns)
31. I feel safe from becoming a victim of crime.	1. Never take this for granted it could make you vulnerable to online scams. (ex) 2. Nobody thinks that it will ever happen to them! Until it does. (rs) 3. Sense of (false) security, especially once past victimisation is forgotten, seems an important aspect (vs) 4. If they have already been a victim they would say no. If never been a victim or someone likely to be a victim they would say yes (ns) 5. Too generic - ranges from petty theft to murder (vs) 6. Not sure people ever believe they will fall victim to a scam! (vs)
32. Only gullible people fall for scams.	1. If you believe this you are setting yourself up for a fall. (ex) 2. A belief which says nothing about the person's actual gullibility (rs) 3. Good question, but I wonder if scam victims would like to describe themselves as gullible. (vs) 4. Maybe a bit direct and strong if you are surveying people who have been scammed - could be taken as offensive (ex)
33. I believe criminals usually end up getting what they deserve.	1. It quickly becomes apparent they don't (ex) 2. Not relevant at all to susceptibility (ex) 3. A belief not a personality characteristic (rs) 3. Unsure how the attitudes of the criminal's consequences are insightful in light of the research context. Unless its an area of inquiry. (rs)
34. Scammers and fraudsters normally will get caught in the end.	1. You are believing that the system is going to look after you (ex) 2. Somewhat relevant but is more important to whether a normal person is tempted to commit an online crime (ex) 3. A belief which says nothing about the person's actual gullibility (rs) 4. Scammers and Fraudsters is better than "criminals" in my opinion and should be used throughout. Eliminates confusion. (rs) 5. My opinion maybe more than anything else! (vs)
35. The Authorities, overall are effective at protecting us from crime.	1. Again if you are naïve thinking that, you are exposed to scams, believing them because the authorities would be doing something about them otherwise (ex) 2. We do our best we can with the resources we currently have but scammers currently have the edge. (ex) 3. Important from an enforcement agency point of view (ex) 4. Not a chance, as we know (vs)
36. People tell me I sometimes make rash decisions.	1. Again making decisions too quickly can lead to falling victim to scams (ex) 2. Somewhat relevant if true (ex)

Question	Comment
37. When I behave impulsively, I normally end up regretting.	1. Do they just not care if they are scammed (ex) 2. If someone learns from a mistake and wants to avoid feelings of regret they are less likely to exhibit risky behaviour. (ex)
38. I don't like to rush my decisions.	1. take your time and you'll find the scammer out (ex) 2. This person is less likely to be susceptible (ex) 3. Even taking a long time, doesn't prevent scamming (ex)
39. I find it hard to say 'no' to people I like.	1. Again implies a relationship with the person (ex) 2. Fraudsters are VERY good at befriending victims (ex) 3. Classic victim (ex) 4. better - especially in face to face, pyramid selling type scams (ex)
40. I tend to believe people I feel I connect with.	1. you've given them an element of your trust (ex) 2. Person highly likely to be scammed. (ex) 3. Very important in terms of fraud via scam mail as they feel that are connected (ex)
41. I have made mistakes when trusting people in the past.	1. Someone who may learn to be more careful after being scammed. (ex) 2. probably applies to everyone (rs) 3.
42. I tend to only buy from companies and brands that I know.	1. How do they know that it is the company or brand that they know this allows the scammer the key to the door if they can pretend to be that company or that product (ex) 2. Good advice if followed. (ex) 3. Very important. I felt compelled to click on a fake 'Apple' site once. (rs)
43. I am always careful to check that emails and websites are real.	1. Nobody does though (ex) 2. Someone who exhibits risk averse behaviour (ex) 3. Very important. (rs) 4. It can be surprisingly difficult to tell (vs)
44. You can never be sure if emails and websites are real.	1. if you have this stance you are looking into the details and less likely to be scammed (ex) 2. Good advice to follow (ex) 3. Sincerity. Once you can fake that, you've got it made. (vs)
45. I am always careful to check out people and companies if I haven't bought from them before.	1. Good but if the scammer is pretending to be somebody or has a good online persona this can be fraught (ex) 2. Good advice (ex) 3. This question if taken literally is asking a lot of people - namely that they check everything. Maybe split or limit to just one (people or companies) (vs) 4. And in my case, I glossed over the warning signs because I wanted to believe. (vs)
46. When something seems too good to be true, it usually is.	1. rule 1 (ex) 2. Always good to keep in mind. (ex)
47. I feel compelled to act immediately when I see a bargain.	1. If you are impulsive you are a scammers dream (ex) 2. This person is highly susceptible (ex)

Question	Comment
48. I get a buzz from buying new things.	1. scammers often use things new to the market so a high risk of being a victim (ex) 2. Potential victim (ex)
49. I am prepared to take a risk when buying something I really want.	1. risk management (ex) 2. This person is at risk (ex)
50. If I like something, I have to have it straight away.	1. Could go either way (ex) 2. At risk (ex) 3. Similar question to other questions (ex)
51. I'm always careful to think rationally about the things I buy.	1. Again pre thought is always a good defence (ex) 2. Someone who believes this is susceptible to being scammed.(ex) 3. Are people likely to see themselves as being irrational? (ex)
52. I find it hard to contain my excitement when lucky things happen to me.	1. Impulsive? (ex) 2. Susceptible (ex) 3. Speaks to impulse control I guess (ex)
53. People sometimes tell me that I am cynical.	1. Defensive, which is good (ex) 2. People should have a healthy cynicism to buying online. (ex)
54. I often try to set myself rules to avoid repeating mistakes.	1. Do we live by rules we've set for ourselves (ex) 2. Maybe less susceptible (ex) 3. Personally, I make and edit all sorts of rule sets for dealing with situations. (vs) 4. Again - is aimed at repeat victims (ex)
55. I try hard to understand the reasons for any mistake I make.	1. A personal issue not relevant to scams (ex) 2. Susceptible (ex) 3. Wisdom comes from analysing your failures, so as not to repeat them. (vs)
56. When I make a mistake, I don't like to dwell on it.	1. As long as you dwell on it long enough not to make the mistake again (ex) 2. Important (ex) 3. Defining the repeat victim??? (vs) 4. Learn from it, then put it behind you. That's not really dwelling. (vs)

Notes.
ex = expert in the field
rs = researcher in the field
vs = victim of scam(s)
ns = never scammed

1.5 Materials used in Study 2, Chapter 4

1.5.1 Susceptibility to Persuasion Scale

Table 1.7
Susceptibility to persuasion scale (Modic & Lea, 2013)

Subscale	Question
Trust and authority	I trust in legal authorities to sort my situation if I was defrauded
	I feel safe and legally protected when buying goods from authority figures
	I trust in information offered to me by authorities
Social influence	I am easily persuaded to do things by my friends
	My friends do not influence me*
	I often follow the crowd even when that is not in my best interest
Self-control	I find it hard to restrain myself from buying things that interest me
	I only buy things when I really need to*
	I cannot easily stop myself from making rash or impulse purchases
Need for consistency	I am not very organised
	I often follow a strict schedule*
	I am often late to meetings despite planning to be on time

Notes.
* reverse item

1.5.2 Scam scenarios

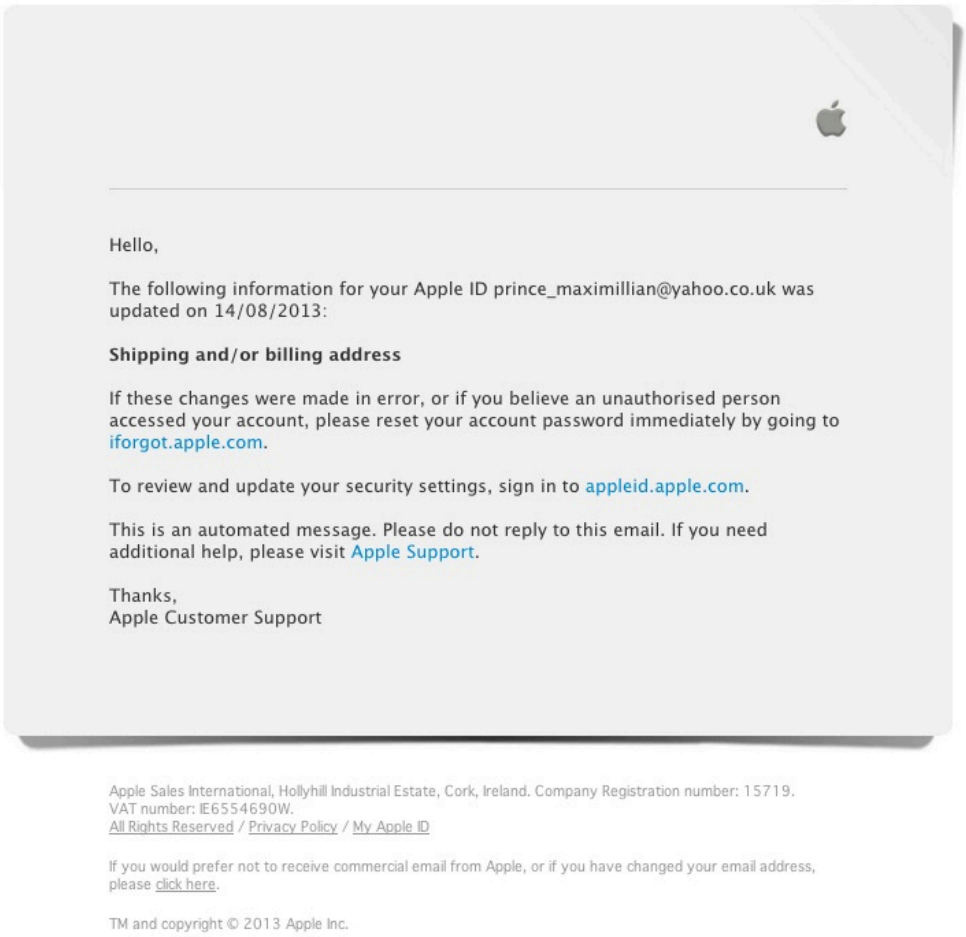
Table 1.8
Scam scenarios adapted from Modic & Lea (2013)

	Type of scam	Scenario
1.	Fake cheque scam	You are selling a quite valuable item through classified ads. You have been trying to sell this for a while. All of a sudden, somebody contacts you and offers to buy this item for the list price. They don't even haggle. They post you a cheque (or check, if you prefer U.S. spelling) and ask you to send the item as soon as possible. You send them the item immediately, wanting to provide a good customer experience. The address is a P.O. Box.) and you send them the item immediately, wanting to provide a good customer experience.
2.	Phishing scam	You receive an email from your bank, notifying you that there was some suspicious activity detected on your account. You should login through a secure link provided and check that everything is in order.
3.	Advance fee, 419 scam	You receive an email from an African or Iraqi relative (you never even knew you had); a Nigerian dictators' wife, a Nigerian building subcontractor, a lawyer, etc. They promise wealth and riches, but require you to cover initial fees in order for the process to successfully conclude. If you have no money, they will sometimes provide you with a check that would cover the initial fees.
4.	Internet auction scam	You found a Lenovo ThinkPad you always wanted on eBay! The sellers feedback is quite high (98% +), they are selling their personal machine and the price is just too good to pass by. You go from wanting to buying it in two minutes, as you know that otherwise somebody else will buy it soon. It is approximately 40% discounted. You want to pay immediately. The seller requires payment through a bank transfer, claiming that PayPal fees are prohibitive. True. Well, you bought it already you might as well pay, if you want to keep your positive feedback score. The bank information sent to you by the seller seems to indicate that you are transferring money to a bank in Hong Kong, but the seller tells you that the goods will be sent from a warehouse in your local country, so that is OK. The seller insists on communicating through personal emails, not through eBay emails, as they "don't want eBay to spy on them". Makes sense.

	Type of scam	Scenario
5.	Investment scam	You are contacted by a stock-broker or their assistant offering an investment opportunity, buying stocks in a company that is the next Google or Shell or ... You are asked to buy stocks and told of huge profits you could make. If you decide to invest, the stocks will actually be bought in your name, but you will not be able to sell them for a set period of time (usually two years).
6.	Pyramid scheme	You are contacted by a midsize business with a great idea on how to make money with a relatively little effort. There is a small charge for an initial 'business pack' that explains everything in detail, but you will be able to make that back very quickly as you recruit helpers, who will also make the initial small payment to you. You will send a small amount out of those payments to your recruiter (for his trouble). Everything else, you will keep. Your recruits will also get to keep most of the money they will make from their recruitments, but will send a small percentage to you. You will earn more and more as the business expands.
7.	In store credit card	You are offered an in-store credit card, from a local well-known retailer. *

Note.
* Not a scam.

1.5.3 Email correspondence stimuli



Hello,

The following information for your Apple ID prince_maximillian@yahoo.co.uk was updated on 14/08/2013:

Shipping and/or billing address

If these changes were made in error, or if you believe an unauthorised person accessed your account, please reset your account password immediately by going to iforgot.apple.com.

To review and update your security settings, sign in to appleid.apple.com.

This is an automated message. Please do not reply to this email. If you need additional help, please visit Apple Support.

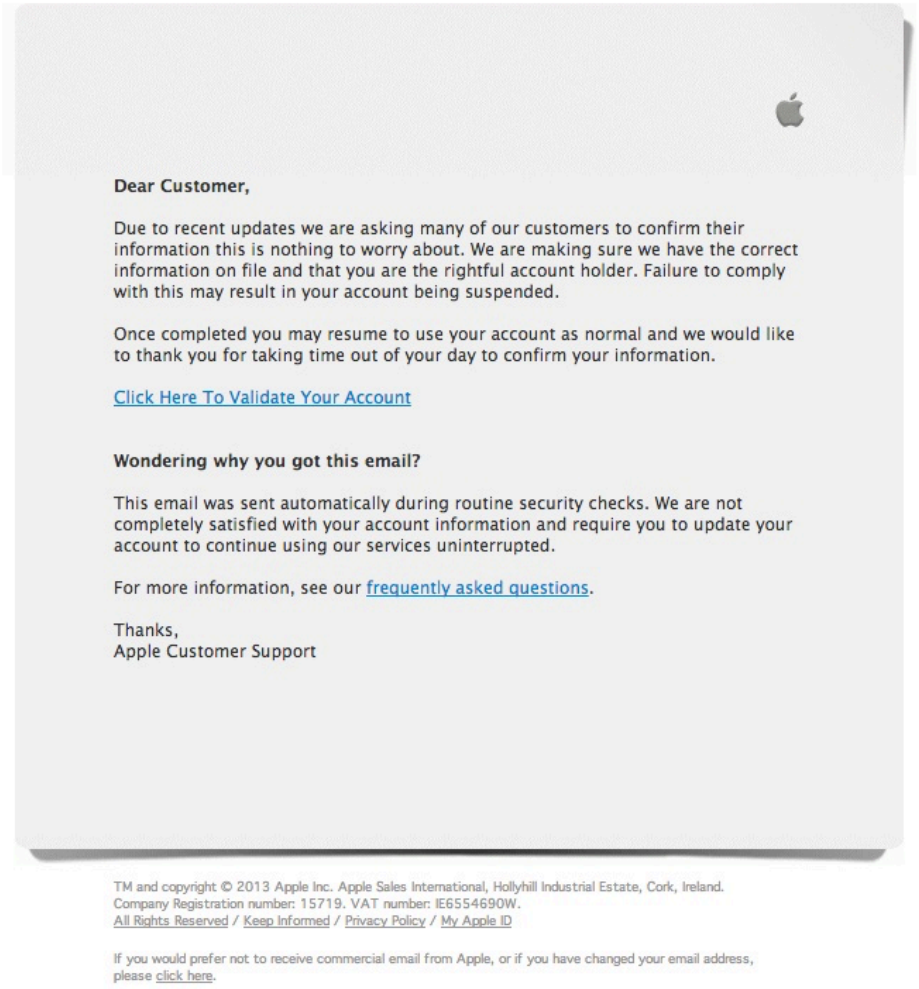
Thanks,
Apple Customer Support

Apple Sales International, Hollyhill Industrial Estate, Cork, Ireland. Company Registration number: 15719.
VAT number: IE6554690W.
All Rights Reserved / Privacy Policy / My Apple ID

If you would prefer not to receive commercial email from Apple, or if you have changed your email address, please click here.

TM and copyright © 2013 Apple Inc.

Figure 1.1 Example of a genuine email correspondence



Dear Customer,

Due to recent updates we are asking many of our customers to confirm their information this is nothing to worry about. We are making sure we have the correct information on file and that you are the rightful account holder. Failure to comply with this may result in your account being suspended.

Once completed you may resume to use your account as normal and we would like to thank you for taking time out of your day to confirm your information.

Click Here To Validate Your Account

Wondering why you got this email?

This email was sent automatically during routine security checks. We are not completely satisfied with your account information and require you to update your account to continue using our services uninterrupted.

For more information, see our frequently asked questions.

Thanks,
Apple Customer Support

Figure 1.2 Example of a phishing email correspondence

1.6 Additional results for Study 2, Chapter 4

1.6.1 Susceptibility to Fraud Scale (STFS)

Table 1.9
Proposed Susceptibility to Fraud Scale, factor description and reliability values

1 – Strongly disagree 2 – Disagree 3 – Neither Agree nor disagree 4 – Agree 5 – Strongly agree

Factor	Questions	Description	Reliability
Compliance	1. I find it hard to say no to people without seeming rude. 2. I normally give in when people pressure me to make a decision. 3. I often find myself agreeing to things I don't really want to do. 4. I find it hard to say no to people I like. 5. People tell me I am easy to persuade. 6. I often worry about disappointing people. 7. When I find myself in a difficult situation I often make decisions I later regret. 8. I would prefer to be impolite rather than agree to something I don't want to do. * 9. I feel others often take advantage of me.	High scores on this factor indicate that the person is more likely to comply with others due to activation of social norms or other factors, such as time pressures, despite awareness of the vulnerability.	α = .87
Vigilance	1. I am always suspicious of people who ask me to make quick decisions. 2. I often double-check what other people tell me. 3. I am always careful to check that emails and websites are real. 4. I am always careful to check out people and companies if I haven't bought from them before. 5. When something seems too good to be true, it usually is.	High scores on this factor indicate awareness of others' motives and readiness to cross check information given.	α = .65
Impulsivity	1. I feel compelled to act immediately when I see a bargain. 2. I get a buzz from buying new things. 3. I am prepared to take a risk when buying something I really want. 4. If I like something, I have to have it straight away.	High scores on this factor indicate lack of restraint and disregard to risk with regards to making purchases	α = .73
Decision time	1. I prefer to take my time to think things through. 2. I prefer to get decisions over with quickly. * 3. People tell me I sometimes make rash decisions. * 4. I don't like to rush my decisions	High scores on this factor indicate a preference to take more time and carefully consider information when making decisions	α = .65
Belief in justice	1. I feel safe from becoming a victim of crime. 2. Only gullible people fall for scams. 3. Scammers and fraudsters normally will get caught in the end. 4. The Authorities, overall are effective at protecting us from crime.	High scores on this factor indicate a perception that justice prevails and people get what they deserve.	α = .48

Note.
* reverse item

1.6.2 Results of the principal axis factoring analysis in Chapter 4

Table 1.10
Factor analysis using principal axis factoring extraction of the 45-item questionnaire

Question	Component				
	1	2	3	4	5
1. I find it hard to say no to people I like.	**.739**				
2. I find it hard to say no to people without seeming rude.	**.735**				
3. I often find myself agreeing to things I don't really want to do.	**.702**				
4. I normally give in when people pressure me to make a decision.	**.681**				
5. People tell me I am easy to persuade.	**.642**				
6. I feel others often take advantage of me.	**.634**				
7. I often worry about disappointing people.	**.580**				
8. I would prefer to be impolite rather than agree to something I don't want to do.	**-.566**				
9. When I find myself in a difficult situation I often make decisions I later regret.	**.505**				
10. I always do what I think is best, even when I am in the minority.	-.447				
11. I tend to believe people I feel I connect with.	.433				
12. I have been talked into buying something I didn't really want.	.406				
13. I find it hard to tell if someone can be trusted.	.390				
14. I usually find it easy to agree with others in a group.	.359				
15. Forceful people make me feel uneasy.	.323				
16. I usually give others the benefit of the doubt.	.320				
17. I don't like to rush my decisions.		**.666**			
18. I prefer to take my time to think things through.		**.566**			
19. People tell me I sometimes make rash decisions.		**-.470**	.334		
20. I prefer to get decisions over with quickly.		**-.433**			
21. I prefer to read contracts for myself rather than believe what others tell me is in them.		.381			
22. I always check the small print.		.368			
23. I often seek advice from friends and family before making financial decisions.					

Question	Component				
	1	2	3	4	5
24. It's not important to read all of the details before making important decisions.					
25. If I like something, I have to have it straight away.			**.678**		
26. I get a buzz from buying new things.			**.627**		
27. I am prepared to take a risk when buying something I really want.			**.593**		
28. I feel compelled to act immediately when I see a bargain.			**.488**		
29. I am always careful to think about things I buy.			-.431		
30. I have made mistakes when trusting people in the past.					
31. I never bother double-checking terms and conditions.					
32. The Authorities, overall are effective at protecting us from crime.				**.436**	
33. I feel safe from becoming a victim of crime.				**.402**	
34. Scammers and fraudsters normally will get caught in the end.				**.397**	
35. Only gullible people fall for scams.				**.351**	
36. I am always careful to check out people and companies if I haven't bought from them before.					**.565**
37. I am always careful to check that emails and websites are real.					**.539**
38. I am always suspicious of people who ask me to make quick decisions.					**.425**
39. I often double-check what other people tell me.					**.377**
40. When something seems too good to be true, it usually is.					**.371**
41. I tend to only buy from companies and brands that I know.					.340
42. I avoid making decisions if someone is pressing me to choose.					.320
43. I normally avoid making decisions when I am feeling anxious.					
44. You can never be sure if emails and websites are real.					
45. I am responsible for deciding what happens to me in every situation.					
Eigenvalues	7.32	3.53	2.37	1.93	1.66
Percentage of variance	16.38	7.85	5.26	4.29	3.70

Notes.
Questions of the Susceptibility to Fraud Scale are shown in bold
Coefficients below .30 not shown

1.7 Additional results for Study 3, Chapter 5

1.7.1 Factor analysis of the STFS using principal axis factoring extraction

Table 1.11
Factor analysis using principal axis factoring extraction of the 26-item Susceptibility to Fraud Scale

Question	Component			
	1	2	3	4
1. I find it hard to say no to people without seeming rude.	.771			
2. I normally give in when people pressure me to make a decision.	.736			
3. I often worry about disappointing people.	.717			
4. I find it hard to say no to people I like.	.685			
5. I often find myself agreeing to things I don't really want to do.	.677			
6. I would prefer to be impolite rather than agree to something I don't want to do.	.570			
7. I feel others often take advantage of me.	.503			
8. People tell me I am easy to persuade.	.495			
9. When I find myself in a difficult situation I often make decisions I later regret.	.457		.328	
10. I am always careful to check out people and companies if I haven't bought from them before.		.564		
11. I prefer to take my time to think things through.		.529	-.359	
12. I am always careful to check that emails and websites are real.		.508		
13. I often double-check what other people tell me.		.458		
14. I am always suspicious of people who ask me to make quick decisions.		.410		
15. When something seems too good to be true, it usually is.		.313		
16. If I like something, I have to have it straight away.			.588	
17. People tell me I sometimes make rash decisions.			-.583	
18. I prefer to get decisions over with quickly.			-.530	
19. I feel compelled to act immediately when I see a bargain.			.487	
20. I don't like to rush my decisions.		.446	-.481	
21. I get a buzz from buying new things.			.352	
22. I am prepared to take a risk when buying something I really want.			.345	
23. Scammers and fraudsters normally will get caught in the end.				.483
24. I feel safe from becoming a victim of crime.				.466

Question	Component			
	1	2	3	4
25. The Authorities, overall are effective at protecting us from crime.				.461
26. Only gullible people fall for scams.				.375
Eigenvalues	5.42	2.62	1.78	1.75
Percentage of variance	20.85	10.07	6.84	6.72

Note.
Coefficients below .30 not shown

1.7.2 Factor analysis of the STFS using principal components extraction

Table 1.12
Factor analysis using principal components extraction of the 26-item Susceptibility to Fraud Scale

Question	Component			
	1	2	3	4
1. I find it hard to say no to people without seeming rude.	.798			
2. I often worry about disappointing people.	.762			
3. I normally give in when people pressure me to make a decision.	.762			
4. I find it hard to say no to people I like.	.735			
5. I often find myself agreeing to things I don't really want to do.	.714			
6. I would prefer to be impolite rather than agree to something I don't want to do.	.644			
7. I feel others often take advantage of me.	.574			
8. People tell me I am easy to persuade.	.553			
9. When I find myself in a difficult situation I often make decisions I later regret.	.504		.344	
10. I am always careful to check out people and companies if I haven't bought from them before.		.667		
11. I am always careful to check that emails and websites are real.		.613		
12. I often double-check what other people tell me.		.589	.357	
13. I prefer to take my time to think things through.		.578	-.394	
14. I am always suspicious of people who ask me to make quick decisions.		.527		
15. When something seems too good to be true, it usually is.		.427		
16. If I like something, I have to have it straight away.			.663	
17. People tell me I sometimes make rash decisions.			-.647	
18. I prefer to get decisions over with quickly.			-.614	
19. I feel compelled to act immediately when I see a bargain.			.580	
20. I don't like to rush my decisions.		.476	-.523	
21. I get a buzz from buying new things.			.456	
22. I am prepared to take a risk when buying something I really want.			.427	
23. Scammers and fraudsters normally will get caught in the end.				.647
24. The Authorities, overall are effective at protecting us from crime.				.617

Question	Component			
	1	2	3	4
25. I feel safe from becoming a victim of crime.				.611
26. Only gullible people fall for scams.				.545
Eigenvalues	5.42	2.62	1.78	1.75
Percentage of variance	20.85	10.07	6.84	6.72

Note.
Coefficients below .30 not shown